La réglementation des traitements de données à caractère personnel concernant le patient dans les hôpitaux

Herveg, Jean

Published in:
Guide hospitalier

Publication date:
2009

Document Version
le PDF de l'éditeur

10.1. La réglementation des traitements de données à caractère personnel concernant le patient dans les hôpitaux

Jean HERVEG ([1])
Centre de Recherches Informatique et Droit
Avocat au barreau de Bruxelles

10.1.1. Objectif de la section

La présente section a pour objectif de fournir les éléments d'information et les outils nécessaires à la bonne application, dans les hôpitaux, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, et plus spécialement en ce qui concerne les données du patient.

10.1.2. Approches fondamentales de la réglementation des traitements de données à caractère personnel

10.1.2.1. La tension fondatrice de la réglementation des traitements de données à caractère personnel

La réglementation des traitements de données à caractère personnel repose sur un double constat, révélateur d'une tension fondatrice qui permet de comprendre la signification et la portée des dispositions légales présentement étudiées.

Le premier constat est celui de la nécessité de traiter des données à caractère personnel, tandis que le second porte sur la nécessité de prendre en compte le sort à réserver à la personne concernée par l'information faisant l'objet d'un traitement. A cet égard, il faut insister sur le fait que la mise en œuvre des droits de la personne concernée ne s'envisage utilement que dans le respect des conditions imposées au responsable du traitement pour le traitement des données à caractère personnel, et inversement.

10.1.2.1.1. La nécessité des traitements de données à caractère personnel

Le premier constat sur lequel repose cette réglementation porte sur la reconnaissance de la nécessité, dans le cours des activités économiques, sociales, culturelles, individuelles et domestiques, sans distinction entre les activités publiques et privées, d'exploiter de l'information relative à des personnes physiques, c'est-à-dire de traiter des données à caractère personnel.

[1] Ce texte a bénéficié de la relecture attentive et des observations judicieuses de Yves Poullet et de Jean-Marc Van Gyseghem. Je les en remercie vivement. Les opinions contenues dans cette contribution n'engagent que leur auteur.

Ainsi, dans les hôpitaux, il est nécessaire, voire indispensable, de traiter des informations relatives au patient afin de lui fournir des soins de santé appropriés et de haut niveau. C'est en principe la raison (finalité) première de l'utilisation des données du patient. A cette fin, elles sont, par exemple :

- créées par le biais des examens médicaux ;
- collectées et structurées dans les dossiers médicaux et infirmiers hospitaliers ;
- consultées, utilisées et communiquées, etc.

Il existe bien entendu de nombreuses autres raisons (finalités), souvent imposées par la loi, qui exigent de traiter les informations relatives au patient au sein d'un hôpital. Ces raisons ressortissent notamment :

- au paiement et au financement des soins de santé,
- au contrôle de la qualité des prestations de soins et du système de santé publique,
- à l'épidémiologie,
- à la recherche scientifique, etc.

En résumé, dans ce premier aspect, la réglementation des traitements de données à caractère personnel prend en compte les intérêts, droits et libertés de la personne désireuse de traiter des données à caractère personnel, soit, en l'espèce, l'hôpital.

10.1.2.1.2. Le sort de la personne concernée

Le second constat sur lequel repose la réglementation des traitements de données à caractère personnel est lié au premier : il faut, en même temps que reconnaître la nécessité de ces traitements, tenir compte de ce qui va advenir de la personne concernée par l'information. Il s'agit ici de prendre en considération les intérêts, droits et libertés de la personne concernée. Cette prise en compte de la personne concernée recouvre deux aspects qui vont de pair.

10.1.2.1.2.1. La protection de la personne concernée

Le premier aspect de la prise en compte de la personne concernée est de nature défensive. Il s'agit de la protéger contre les risques qui peuvent découler de l'usage qui peut être fait de cette information. Il faut la protéger contre toute atteinte à ses intérêts, droits et libertés, qui pourrait résulter du traitement de l'information qui la concerne.

Pour prendre un exemple, la communication d'informations relatives à la santé du patient à des personnes « non autorisées » est de nature à l'exposer à des risques de discrimination à l'emploi, au crédit, au logement, etc. De même, le contrôle de la qualité des soins implique de traiter de l'information relative au praticien concerné, ce qui est également de nature à l'exposer à des risques en termes d'emploi. Il s'agit donc de prendre les mesures appropriées pour prévenir l'avènement de ces conséquences indésirables.

En droit, cette protection s'exprime au travers des conditions imposées au responsable du traitement pour qu'il puisse traiter des données à caractère personnel sans porter atteinte aux intérêts, droits et libertés de la personne concernée. Concernant les données médicales, cette protection s'exprime par une interdiction de traitement sauf exceptions.

10.1.2.1.2.2. L'autodétermination informationnelle de la personne concernée

Le second aspect de la prise en compte de la personne concernée est de nature plus dynamique. Il s'agit d'assurer son droit à la maîtrise de son image informationnelle, c'est-à-dire, en quelques mots, son droit de savoir ce qui est su d'elle et ce qui en est fait, ainsi que de pouvoir influer sur l'usage de l'information qui la concerne. Dans la réglementation, cette maîtrise se manifeste au travers des droits reconnus à la personne concernée lors du traitement de l'information qui la concerne.

Ainsi, par exemple, la personne concernée, que ce soit le patient ou un membre du personnel de l'hôpital, peut consentir au traitement de données à caractère personnel qui la concerne. Elle dispose aussi d'un droit d'accès, de rectification, et d'opposition.

Il s'agit donc de prendre les mesures appropriées pour garantir ce droit à la maîtrise de son image informationnelle, cette « autodétermination informationnelle ».

10.1.2.1.3. En résumé

Le traitement d'informations relatives à des personnes physiques est très fréquemment nécessaire, voire indispensable, pour de multiples raisons. Mais, en même temps, le fait d'utiliser cette information induit le danger d'exposer les personnes concernées à des risques de discrimination ou d'atteintes à leurs droits et libertés, tout en mettant en jeu leur maîtrise sur leur image informationnelle. Il ne s'agit donc pas de soutenir que les traitements de données à caractère personnel seraient réglementés en raison du seul fait qu'ils concerneraient des données intimes ou cachées, même si l'intimité de la personne concernée est assurément un intérêt à protéger.

Par voie de conséquence, c'est à cet effet et dans cette optique que les traitements de données à caractère personnel doivent respecter toute une série de règles qui visent à atteindre un équilibre acceptable entre les intérêts en présence. A cet égard, si c'est bien la confrontation entre les intérêts du responsable du traitement et ceux de la personne concernée qui constituent le principe de la tension paradoxale sous-jacente à la réglementation des traitements de données à caractère personnel, il n'en demeure pas moins que ces deux catégories d'intérêts s'inscrivent dans un contexte plus global qui explique et justifie que soient également pris en compte les intérêts de la collectivité et des tiers considérés individuellement. Il s'ensuit que l'appréciation de la légitimité à traiter des données à caractère personnel implique de prendre en considération non seulement les intérêts du

responsable du traitement et de la personne concernée, mais également ceux de la collectivité et des tiers considérés individuellement, sauf à isoler les deux premiers des contraintes de la vie en société.

Il faut en outre insister sur le fait que la règlementation des traitements de données à caractère personnel ne concerne pas que le patient, mais aussi toutes les personnes œuvrant au sein de l'hôpital.

10.1.2.2. Les fondements juridiques de la réglementation des traitements de données à caractère personnel

La réglementation des traitements de données à caractère personnel obéit à la tension paradoxale qui la sous-tend. D'un côté, il faut permettre les traitements de données à caractère personnel. De l'autre côté, il faut tenir compte du sort de la personne concernée. Par voie de conséquence, la détermination des fondements juridiques de la réglementation des traitements de données à caractère personnel consiste à dégager les fondements juridiques dont peuvent se prévaloir les deux branches de cette tension paradoxale.

10.1.2.2.1. Le fondement juridique dans le chef du responsable du traitement

Du côté du responsable du traitement, le fondement juridique de son intérêt ([2]) doit être recherché dans ce qui justifie l'activité projetée à laquelle est liée la nécessité de traiter des données à caractère personnel. Ainsi, pour une entreprise, il s'agira dans la plupart des cas de la liberté d'entreprendre. Pour une collectivité politique, il s'agira de la réalisation de ses missions d'intérêt public. Pour un hôpital, il s'agira de la réalisation de son objet social et des missions, bien souvent de service public, qui, en outre, peuvent lui être imparties par la loi.

10.1.2.2.2. Le fondement juridique dans le chef de la personne concernée

De l'autre côté, la prise en compte du sort de la personne concernée dans le traitement des données à caractère personnel part du principe selon lequel l'individu a le droit de mener sa vie librement sans ingérence injustifiée, que ce soit à l'égard des autorités publiques ou des autres personnes privées. A cet effet, la personne doit être prémunie contre les risques de discrimination et d'atteinte à ses droits et libertés, tout en se voyant reconnaître les moyens de pouvoir agir sur l'information qui la concerne. Parmi les nombreux risques d'ingérence injustifiée qui sont susceptibles de peser sur les individus, ceux qui sont liés aux traitements de données à caractère personnel ont spécialement retenu l'attention en raison des développements considérables des nouvelles technologies de l'information et de la communication dans tous les secteurs d'activités, sans préjudice du danger déjà représenté par le fichage manuel des individus ([3]).

---

2 Serait-il possible de dire qu'il est titulaire d'un droit ou d'une liberté à traiter des données ?

3 Sur les risques présentés par les nouvelles technologies, voyez déjà en matière de :

Le secteur des soins de santé n'a évidemment pas échappé à ce constat et, en la matière, une des préoccupations majeures consiste à protéger la personne concernée contre les ingérences indues qui résulteraient du traitement de données à caractère personnel relatives à sa santé tout en lui conférant les instruments lui permettant d'agir sur l'information qui la concerne. Pour reprendre l'exemple de la communication « non autorisée » de données médicales, celle-ci est de nature à exposer le patient à des risques de discrimination à l'emploi, à l'assurance ou au crédit, tout en constituant une ingérence injustifiée dans sa maîtrise sur ce qui est su à propos de son état de santé. Par ailleurs, le droit d'accès du patient à ses données médicales lui permet notamment de mieux apprécier son état de santé, ce qui est nécessaire à la conduite de sa vie.

10.1.2.2.2.1. Le droit au respect de la vie privée

Traditionnellement, la prise en compte de la personne concernée dans le traitement de données à caractère personnel a été construite à partir du droit au respect de la vie privée ([4]).

- profilage : Council of Europe, T-PD, Report on the application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee, by J.M. DINANT, Chr. LAZARO, Y. POULLET, N. LEFEVER et A. ROUVROY, T-PD(2008)01, 11 January 2008;
- données biométriques : Council of Europe, T-PD, Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005);
- cartes à puce : Council of Europe, Guiding principles for the protection of personal data with regard to smart cards (2004); T-PD, Report on the protection of personal data with regard to the use of smart cards (2001), by Mr Karel NEUWIRT;
- www : Council of Europe, T-PD, Report on the application of data protection principles to the worldwide telecommunication networks, by Prof. Yves POULLET and its Team (2004);
- nouvelles techniques de surveillance : Council of Europe, Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (2003); Council of Europe, T-PD, Protection of personal data with regard to surveillance (2000) and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance, by Mr. Giovanni BUTTARELLI;
- flux transfrontières : Council of Europe, T-PD, Study contracts involving the transfer of personal data between Parties to Convention Ets 108 and third countries not providing an adequate level of protection (2001), by Mr. Jérôme HUET.

[4] Article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. La Charte des droits fondamentaux de l'Union européenne (*J.O.U.E.*, 14 déc. 2007, C 303/01) énonce également que « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* » (art. 7). Le Praesidium de la Convention qui a élaboré la Charte explique que les droits garantis à l'article 7 correspondent à ceux qui sont garantis par l'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, mais que pour tenir compte de l'évolution technique, le mot « communication » a été substitué à celui de correspondance (Explications relatives à la charte des droits fondamentaux, *J.O.U.E.*, 14 déc. 2007, C 303/17, spéc. C 303/20). Sur le lien entre le droit au respect de la vie privée et la protection des données, voyez not. : H. BURKERT, « Dualities of Privacy – An Introduction to « Personal Data Protection and Fundamental Rights », Bruxelles, à paraître ; S. CALLENS, « La « société de l'information » : une société de surveillance ? », in M. MATHIEN (dir.), *La « Société de l'Information ». Entre mythes et réalités*, Collection Médias, Sociétés et Relations Internationales, Bruxelles, Bruylant, 2005, p. 205 ; J.E. COHEN, « Privacy, Visibility, Transparency and Exposure », *The University of Chicago Law Review*, 2005, p. 181 ; C. JUGASTRU, « La protection des données personnelles et le commerce

En effet, le droit au respect de la vie privée assure une protection générale à l'individu contre toute ingérence injustifiée dans la façon dont il entend mener sa vie. Cette protection générale de l'individu est fondamentale dans la mesure où elle permet l'exercice des autres libertés. En effet, sans cette liberté d'agir sans ingérence indue, les autres libertés n'ont que fort peu de signification ou d'intérêt.

Pour ce qui nous concerne, le droit au respect de la vie privée protège l'individu contre les ingérences, ou plus précisément, contre les risques de discrimination ou d'atteinte à ses droits et libertés, qui pourraient advenir à l'occasion du traitement de données à caractère personnel, tout en lui offrant les instruments nécessaires pour agir à l'égard de l'information qui le concerne.

La Cour européenne des droits de l'homme a déjà eu l'occasion de souligner l'importance de la protection des données à caractère personnel, et en particulier des données médicales, pour l'exercice du droit au respect de la vie privée, dans ses arrêts du 25 février 2007 (Z. c Finlande), du 27 août 2007 (M.S. c Suède) et du 17 juillet 2008 (I. c Finlande). Dans ce troisième arrêt, la Cour a répété l'enseignement déjà affirmé dans les deux précédents, et selon lequel :

> « 38. La protection des données à caractère personnel, et spécialement des données médicales, revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention. Le respect du caractère confidentiel des informations sur la santé constitue un principe essentiel du système juridique de toutes les Parties contractantes à la Convention. **Il est capital non seulement pour protéger la vie privée des malades mais également pour préserver leur confiance dans le corps médical et les services de santé** ([5]) en général. (…) La législation interne doit ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention (…) ».

électronique – La situation en droit roumain », in Fr. PERON (coord.), *L'Europe dans la société de l'information*, Bruxelles, Larcier, 2008, p. 187 ; Th. LEONARD et Y. POULLET, « Les libertés comme fondement de la protection des données nominatives », in Fr. RIGAUX, *La vie privée. Une liberté parmi les autres ?*, Travaux de la faculté de droit de Namur, n° 17, Bruxelles, Larcier, 1992, p. 231 ; Y. POULLET, « Le fondement du droit à la protection des données nominatives : « Propriétés ou libertés », in *Nouvelles technologies et propriété*, Paris, Ed. Thémis, 1991, p. 175 ; « Data Protection between Property and Liberties. A Civil Law Approach », in *Amongst Friends in Computers and Law, A collection of Essays in Remembrance of Guy Vandenberghe*, Deventer-Boston, Kluwer Law and Taxation Publishers, 1990, p. 161; "La protection des données: entre libertés, droits subjectifs et intérêts légitimes", in *Liber Amicorum Paul Martens. L'humanisme dans la résolution des conflits. Utopie ou réalité ?* Bruxelles, Larcier, 2007, p. 133 ; P. TABATONI (dir.), *La protection de la vie privée dans la société de l'information*, Cahier des sciences morales et politiques, 5 tomes, Presses universitaires de France, 2000 ; Fr. RIGAUX, "La protection des banques de données et le respect de la vie privée", *rev. dr. ULB*, 1994, p. 51 ; M. VAN OVERSTRAETEN et S. DEPRE, « Le traitement automatisé de données à caractère personnel et le droit au respect de la vie privée en Belgique », *rev. trim. dr. h.*, 54/2003, p. 665.

[5] Nous soulignons.

10.1.2.2.2.2. Le droit à la protection des données à caractère personnel

Après avoir été construit sur la base du droit au respect de la vie privée, le droit à la protection des données à caractère personnel a été formellement consacré en tant que tel par la Charte des droits fondamentaux de l'Union européenne ([6]) dans une disposition distincte de celle qui concerne le droit au respect de la vie privée ([7]). Le Praesidium de la Convention, qui a élaboré la Charte, a énuméré les bases de cette nouvelle disposition. Parmi celles-ci se retrouvent l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales ainsi que les principaux instruments juridiques européens qui ont été adoptés dans son giron pour assurer la protection des citoyens à l'égard des traitements de données à caractère personnel ([8]).

Il se confirme dès lors bien des précisions apportées par le Praesidium que ce droit nouvellement formalisé à la « *protection des données à caractère personnel* » s'enracine fermement et profondément dans le terreau du droit au respect de la vie privée et que le fait de l'avoir inscrit dans une disposition séparée n'a pas pour but ni pour conséquence de couper ce lien fondamental entre la règlementation des traitements de données à caractère personnel et le droit au respect de la vie privée ([9]).

10.1.3. La réglementation des traitements de données à caractère personnel dans les hôpitaux

Il existe d'innombrables instruments juridiques susceptibles d'intéresser les traitements de données à caractère personnel dans les hôpitaux. Au niveau international, les principaux instruments sont :

- l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales ;

---

6 La Charte des droits fondamentaux de l'Union européenne a été publiée au Journal officiel des Communautés européennes le 18 décembre 2000 (C 364/1). A son sujet voyez déjà : les communications de la Commission du 13 septembre 2000 sur la Charte (COM(2000) 559 final) ; du 11 octobre 2000 sur la nature de la charte (COM(2000) 644 final) ; du 27 avril 2005 sur le respect de la charte dans les propositions législatives de la Commission (Méthodologie pour un contrôle systématique et rigoureux) (COM(2005) 172 final) ; ainsi que les explications relatives à la Charte parue au Journal officiel de l'Union européenne le 14 décembre 2007 (C 303/17).

7 Article 8 de la charte des droits fondamentaux de l'Union européenne :

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

8 Explications relatives à la charte des droits fondamentaux, *J.O.U.E.*, 14 déc. 2007, C 303/17.

9 A ce sujet, voyez not. : Y. POULLET, "La protection des données: entre libertés, droits subjectifs et intérêts légitimes", o.c., p. 142.

- la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 ;
- les Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, adoptés par l'assemblée générale des Nations-Unies dans sa résolution 45/95 du 14 décembre 1990 ;
- la Directive 95/46/EC du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;
- le Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, *J.O.C.E.*, L 8/1 du 12 janvier 2001 ;
- la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.C.E.*, L 201/37 du 31 juillet 2002 (pour la version consolidée, voyez le document 2002L0058-FR-03.05.2006-001.001) ;
- la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.U.E.*, L 105/54 du 14 avril 2006 ;
- auquel il convient d'ajouter maintenant l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

Au sein de l'ordre juridique belge, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel constitue la base de la réglementation des traitements de données à caractère personnel ([10]). Elle a été exécutée par l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. C'est cette législation qui va retenir principalement notre attention, et plus particulièrement sa mise en œuvre qui se présente comme suit :

- Identification des traitements de données à caractère personnel ;
- Identification des différents acteurs qui sont susceptibles d'intervenir dans les traitements de données à caractère personnel ;
- Déterminer les conditions générales de licéité des traitements de données à caractère personnel ;
- Déterminer les droits de la personne concernée par le traitement de données à caractère personnel ;

---

[10] Voyez en ce sens : C.A., arrêt n° 162/2004 du 20 octobre 2004.

- Déterminer les obligations en termes de confidentialité et de sécurité des traitements de données à caractère personnel ;
- Déclaration des traitements de données à caractère personnel auprès de la Commission de protection de la vie privée ;
- Transferts de données à caractère personnel hors Union européenne ;
- La Commission de la protection de la vie privée et les Comités sectoriels ;
- Les sanctions pénales.

Nous terminerons par un très bref aperçu des règles en matière de communications électroniques et de caméras de surveillance.

10.1.3.1. Identification des traitements de données à caractère personnel

Identifier les traitements de données à caractère personnel revient à définir le champ d'application matériel et territorial de la loi du 8 décembre 1992.

10.1.3.1.1. Le champ d'application matériel de la loi du 8 décembre 1992

La loi du 8 décembre 1992 s'applique à (art. 3, § 1er, de la loi du 8 décembre 1992) :

- tout traitement de données à caractère personnel automatisé en tout ou en partie ;
- tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

La définition de ces termes appelle quelques développements.

Il faudra ensuite préciser les limites du champ d'application matériel de la loi du 8 décembre 1992.

10.1.3.1.1.1. La notion de données à caractère personnel

La loi du 8 décembre 1992 définit la notion de « données à caractère personnel » comme étant toute information concernant une personne physique identifiée ou identifiable (la « personne concernée ») (art. 1er, § 1er, de la loi du 8 décembre 1992).

Elle précise que la personne concernée est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale (art. 1er, § 1er, de la loi du 8 décembre 1992).

La définition des données à caractère personnel est essentielle à la bonne application de la loi, ce qui explique que l'accent soit mis sur plusieurs de ses aspects ([11]).

10.1.3.1.1.1.1. Toute information

D'abord, la notion de « données à caractère personnel » vise toute sorte d'information et pas seulement celle qui révèlerait la personnalité de la personne concernée ou qui relèverait de la notion plus restreinte d'information secrète, cachée, et sans qu'il soit requis d'opérer une distinction entre des activités publiques ou privées.

Il s'agit d'opter pour la définition la plus large du concept de « données à caractère personnel ». Ces dernières englobent n'importe quelle information sous n'importe quel format, alphabétique, numérique, graphique, photographique ou acoustique. Les sons et les images sont dès lors des données à caractère personnel dans la mesure où elles représentent des informations qui concernent une personne physique (identifiée ou identifiable).

Le groupe 29 souligne les deux rôles que peuvent remplir les données biométriques (par exemple, les données ADN). Elles peuvent :

- soit contenir de l'information,
- soit servir d'identificateur.

Le groupe 29 ajoute à cet égard que les prélèvements de sang (ou tout autre prélèvement de tissus ou cellules humains) ne sont pas des données biométriques mais constituent des sources d'information dont on peut extraire des données biométriques. Il s'ensuit que l'extraction d'informations concernant une personne physique identifiée ou identifiable à partir de ces prélèvements est assimilée à une collecte de données à caractère personnel.

10.1.3.1.1.1.2. Concernant une personne physique

Ensuite, l'information doit « concerner » une personne physique. Le groupe 29 a identifié trois éléments qui permettent de savoir si cette exigence est rencontrée. Elle doit présenter soit un élément de « **contenu** », soit un élément de « **finalité** », soit un élément de « **résultat** », étant entendu que la présence d'un seul de ces critères suffit pour être en présence d'une information qui concerne une personne ([12]).

> S'agissant du critère de « **contenu** », il signifie que l'information concerne une personne physique parce qu'elle a trait à cette personne. Par exemple, les résultats

---

[11] Les développements qui suivent reprennent ou se fondent principalement sur ceux du Groupe de travail « article 29 » sur la protection des données, Avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007, WP 136.

[12] Il n'est pas sûr que les critères dégagés par le groupe 29 soient exempts de toute critique. Ainsi, il est permis de se demander s'il subsiste des données qui ne seraient pas à caractère personnel.

d'une analyse médicale ont trait au patient ; elles le concernent sans aucun doute au vu de leur contenu informationnel.

S'agissant du critère de « **finalité** », il signifie que l'information concerne une personne physique parce que les données sont utilisées ou susceptibles d'être utilisées, compte tenu de l'ensemble des circonstances du cas d'espèce, afin d'évaluer, de traiter d'une certaine manière ou d'influer sur le statut ou le comportement d'une personne physique.

S'agissant du critère de « **résultat** », il signifie que l'information concerne une personne physique parce que, même en l'absence de tout élément de «contenu» ou de «finalité», on peut considérer que l'information «concerne» une personne physique lorsque son utilisation est susceptible d'avoir un impact sur certains droits ou intérêts de cette personne, compte tenu de l'ensemble des circonstances du cas d'espèce. Il convient de relever qu'il n'est pas nécessaire que le résultat potentiel ait un impact majeur. Il suffit qu'une personne physique puisse être traitée différemment par rapport à d'autres personnes à la suite du traitement de ces données ([13]).

Dans ces conditions, il n'est pas impossible qu'une même information puisse concerner plusieurs personnes à la fois, ce qui risque d'être souvent le cas avec les données médicales et les données génétiques ([14]).

10.1.3.1.1.1.3. Identification de la personne concernée

a. Principe

Pour qu'il ait « donnée à caractère personnel », la personne physique concernée par l'information faisant l'objet d'un traitement doit être *identifiée* ou *identifiable*.

Le fait d'être ***identifié*** signifie que la personne est distinguée des autres membres du groupe auquel elle appartient.

Le fait d'être ***identifiable*** signifie que la personne n'est pas encore identifiée mais qu'il est possible de le faire, que ce soit directement ou indirectement. A cet égard, il importe de rappeler que l'identification s'opère normalement grâce à des « identifiants » (dont certains sont repris dans la définition légale). Comme le précise le groupe 29, il peut s'agir de signes extérieurs concernant l'apparence de la personne comme sa taille, la couleur de ses cheveux,

---

[13] Voyez l'exemple des RFID : Groupe de travail « article 29 » sur la protection des données, «Document de travail sur les questions de protection des données liées à la technologie RFID», adopté le 19 janvier 2005, WP 105, p. 9.

[14] J.-M. VAN GYSEGHEM, « L'information génétique et le traitement de données à caractère personnel », in A.-M. DUGUET, J. HERVEG et I. FILIPPI (éd.), *Dossier Médical et Données Médicales de Santé: Protection de la confidentialité, conditions d'accès, échanges pour les soins et la recherche*, Bordeaux, Les éditions hospitalières, 2007, pp. 243-258.

ses vêtements, etc., ou d'une caractéristique de la personne qui n'est pas immédiatement perceptible, comme une profession, une fonction, un nom, etc. Il peut aussi s'agir d'un numéro de téléphone, d'un numéro de plaque minéralogique, d'un numéro de sécurité sociale, d'un numéro de passeport, ou par un croisement de critères significatifs, qui permettent de reconnaître la personne à l'intérieur d'un petit groupe.

Le groupe 29 souligne le fait que c'est le contexte du cas d'espèce qui déterminera si certains identifiants sont suffisants pour permettre l'identification. Ainsi, un nom de famille très courant ne sera pas suffisant pour identifier une personne − c'est-à-dire pour la distinguer des autres − dans l'ensemble de la population d'un pays, alors qu'il sera probablement suffisant pour identifier un élève dans une classe. La question de savoir si une personne à laquelle se rapportent les informations est identifiée ou pas, dépend dès lors des circonstances de chaque cas d'espèce.

Ceci étant, la possibilité que la personne concernée soit identifiable doit s'envisager de façon raisonnable. Autrement dit, pour déterminer si la personne concernée est identifiable, il faut prendre en considération l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par toute autre personne, pour réaliser cette identification ([15]). A cet effet, il faut tenir compte de tous les facteurs à disposition pour réaliser cette identification, ce qui vise notamment :

- les coûts de l'identification,
- la finalité visée (lorsque la finalité implique l'identification de personnes physiques ([16])),
- la manière dont le traitement est structuré,
- l'intérêt escompté par le responsable du traitement,
- les intérêts en jeu pour les personnes,
- les risques de dysfonctionnements organisationnels (par exemple violations du devoir de confidentialité),
- les défaillances techniques, etc.

b. Prise en considération de l'évolution technologique

Le groupe 29 considère que l'appréciation du caractère raisonnable doit tenir compte de l'état d'avancement technologique au moment du traitement, ce qui est évident, mais aussi des changements technologiques éventuels pendant la période pour laquelle les données seront traitées, ce qui l'est moins. Autrement dit, l'identification peut ne pas être raisonnablement possible aujourd'hui, mais, si les données sont destinées à être conservées pendant une longue durée, le responsable du traitement devrait envisager la possibilité qu'une identification puisse intervenir au cours de cette durée, ce qui en ferait à ce moment-là des données à caractère

---

15 Considérant n° 26 de la directive 95/46/CE.

16 Le groupe 29 considère qu'il s'agit d'un critère très important même s'il n'est pas certain que cette approche soit toujours logique.

personnel. Il serait alors souhaitable que le système puisse s'adapter à ces développements et intégrer les mesures techniques et organisationnelles appropriées en temps utile. Cela ne signifie pas pour autant qu'il faille considérer que les données soient à caractère personnel dès le début.

c. Exemples

Le groupe 29 donne deux exemples en matière d'identification qui sont susceptibles de nous intéresser.

c.1. Publication de clichés radiographiques portant le prénom d'une patiente

Le cliché radiographique d'une patiente a été publié dans un journal scientifique, associé au prénom de celle-ci, un prénom très rare. Le prénom de cette personne associée à la connaissance qu'avaient ses proches de l'affection dont elle souffrait rendaient cette personne identifiable à un certain nombre de personnes; ce cliché radiographique entre alors dans la catégorie des données à caractère personnel.

c.2. Données de recherche pharmaceutique

Les hôpitaux ou les médecins, à titre individuel, transfèrent des informations médicales concernant leurs patients à une société à des fins de recherche médicale. Aucun nom de patient n'est utilisé, mais seulement un numéro de série attribué de manière aléatoire à chacun des cas cliniques, afin d'assurer la cohérence et d'éviter toute confusion avec des informations concernant différents patients. Seuls les médecins, qui sont tenus au secret médical, sont en possession des noms de leurs patients. Les données ne contiennent aucune autre information susceptible de rendre les patients identifiables par recoupement. De plus, toutes les autres mesures ont été prises pour éviter que les personnes concernées puissent être identifiées ou deviennent identifiables, que ce soit sur le plan juridique, technique ou organisationnel. Dans ces circonstances, l'autorité chargée de la protection des données peut considérer qu'il n'existe aucun moyen, dans le cadre du traitement des données réalisé par la société pharmaceutique, susceptible d'être raisonnablement mis en œuvre pour identifier les personnes concernées.

Lorsque l'identification de la personne concernée ne figure pas dans la finalité du traitement, la mise en place des mesures techniques et organisationnelles pour prévenir l'identification peut être déterminante pour considérer que les personnes ne sont pas identifiables, compte tenu de l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par toute autre personne, pour réaliser cette identification. Dans ce cas, la mise en œuvre de ces mesures ne s'inscrit pas dans les mesures techniques et organisationnelles à prendre pour assurer la confidentialité et la sécurité du traitement de

données. Il s'agit en réalité d'un des éléments qui permettent de considérer que les informations ne sont pas des données à caractère personnel ([17]).

d. La pseudonymisation, les données codées et les données anonymes

Le groupe 29 nous envisage ensuite les exemples de la pseudonymisation, des données codées et des données anonymes.

d.1. La pseudonymisation

La pseudonymisation est un traitement de données qui consiste à dissimuler l'identité de la personne concernée. L'objectif de ce traitement est de permettre la collecte de données supplémentaires relatives à cette même personne sans qu'il soit nécessaire de connaître son identité. C'est un aspect particulièrement important dans le contexte de la recherche et des statistiques.

La pseudonymisation peut s'effectuer de manière retraçable en utilisant :

- soit des listes de correspondance des identités et de leurs pseudonymes,
- soit des algorithmes de cryptage à double sens pour la pseudonymisation.

Les données pseudonymisées de manière retraçable sont des données à caractère personnel puisqu'il s'agit d'informations qui concernent des personnes physiques (indirectement) identifiables, les pseudonymes permettant d'établir une correspondance avec la personne concernée.

L'efficacité de la procédure de pseudonymisation dépend d'un certain nombre de facteurs :

- le stade auquel on y recourt,
- son niveau de sécurité en ce qui concerne la possibilité de retracer les informations,
- l'importance de la population dans laquelle la personne est dissimulée,
- la possibilité de rattacher des transactions ou des enregistrements individuels à une même personne, etc.,
- les pseudonymes doivent faire l'objet d'un choix aléatoire et non prévisible,
- la quantité de pseudonymes possible doit être assez grande pour que le même pseudonyme ne puisse jamais être choisi deux fois au hasard. Pour garantir un niveau de sécurité élevé, il importe que l'ensemble des pseudonymes potentiels soit au moins équivalent à l'éventail des valeurs des fonctions de hachage cryptographique sûres.

---

[17] L'observation qui peut être formulée à cet égard consiste à souligner le fait que suivant la finalité, la donnée serait ou non à caractère personnel. Il n'est pas sûr que cette approche soit cohérente.

Par ailleurs, il est possible de dissimuler l'identité des personnes concernées de manière à rendre toute réidentification impossible, par exemple, grâce à un cryptage à sens unique dont il est actuellement toujours considéré qu'il génère des données anonymisées.

d.2. Les données codées

Les données codées sont un exemple classique de pseudonymisation. Les informations correspondent à des personnes physiques possédant chacune un code, la clé permettant d'établir une correspondance entre ce code et des identifiants courants de ces personnes physiques comme le nom, la date de naissance, l'adresse, ces identifiants étant conservée séparément.

Ce type de données est couramment utilisé dans les essais cliniques de médicaments. En général, l'investigateur collecte des données sur les résultats cliniques des participants qui sont identifiés chacun par un code. Le chercheur ne communique les informations à la société pharmaceutique ou à d'autres parties intéressées (les «promoteurs») que sous forme codée. L'investigateur conserve séparément la clé permettant d'associer le code aux identifiants qui permettent d'identifier les participants, ce qui permet de mettre à jour ou de compléter les données collectées, de prévenir le participant de la survenance d'effets secondaires, d'un diagnostic ou de la possibilité d'un traitement médical pour améliorer son état de santé.

Toute la question est de savoir si les données concernent des personnes identifiables. Un premier critère à mettre en œuvre est celui de la finalité du traitement des données codées. En effet, à suivre le groupe 29, si l'une des finalités est de permettre l'identification des participants, notamment pour l'un des motifs énoncés ci-avant, nous serons bien entendu en présence de données à caractère personnel. Le groupe 29 note à cet égard que lorsque le promoteur a analysé les moyens destinés au traitement, qu'il a prévu les mesures organisationnelles et ses relations avec le chercheur qui détient la clé de manière telle que l'identification des personnes concernée *peut* non seulement intervenir, mais *doit* aussi intervenir dans certaines circonstances, il s'ensuit que l'identification des patients figure parmi les finalités et les moyens du traitement. Par voie de conséquence, dans ce cas de figure, les données codées constituent des informations concernant des personnes physiques identifiables par toutes les parties concernées par l'identification éventuelle, et sont soumises aux règles de protection des données. Mais le groupe 29 précise, à juste titre, que cela ne signifie pas pour autant que tout autre responsable du traitement des données qui traite le même ensemble de données codées doive être considéré comme traitant des données à caractère personnel, notamment lorsque le système spécifique dans lequel ces autres responsables du traitement des données codées opèrent, exclut expressément la réidentification et que des mesures techniques ont été prises à cet effet.

Le groupe 29 ajoute que dans d'autres domaines de la recherche ou dans le cadre d'un même projet, il est possible que la réidentification de la personne concernée ait été exclue lors de la conception des protocoles et de la procédure, par exemple lorsqu'aucun aspect thérapeutique

n'est concerné. Pour des raisons techniques ou autres, il peut toujours être possible de découvrir à quelles personnes correspondent telles données cliniques, mais cette identification n'est en aucun cas censée se produire ou escomptée, et des mesures techniques appropriées (par exemple cryptographie, hachage irréversible) ont été mises en place pour prévenir cette éventualité. Dans ce cas, même si l'identification de certaines personnes concernées peut se produire malgré tous les protocoles et mesures (en raison de circonstances imprévisibles telles qu'une correspondance accidentelle des caractéristiques de la personne concernée qui révèlent son identité), les informations traitées par le responsable initial peuvent ne pas être considérées comme concernant des personnes physiques identifiées ou identifiables, compte tenu de l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par toute autre personne. Leur traitement peut ainsi ne pas être soumis à la réglementation des traitements de données à caractère personnel. Il en va tout autrement pour le nouveau responsable du traitement qui a effectivement eu accès aux données identifiables qui seront, elles, sans aucun doute considérées comme des «données à caractère personnel».

L'arrêté royal du 13 février 2001 définit les données à caractère personnel codées comme étant les données à caractère personnel qui ne peuvent être mises en relation avec la personne identifiée ou identifiable que par l'intermédiaire d'un code (art. 1er, 3°, de l'arrêté royal du 13 février 2001).

d.3. Les données anonymes

Une donnée anonyme est toute information qui concerne une personne physique qui ne peut pas être identifiée, ni par le responsable du traitement des données ni par toute autre personne, compte tenu de l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par toute autre personne, pour procéder à cette identification.

La donnée anonymisée est une donnée anonyme qui concernait auparavant une personne identifiable mais qu'il n'est plus possible d'identifier.

De nouveau, il faut tenir compte des circonstances propres à chaque cas d'espèce et un examen au cas par cas s'impose. Il faut vérifier les moyens susceptibles d'être raisonnablement mis en œuvre pour réaliser l'identification de la personne concernée.

A cet égard, le groupe 29 souligne le fait que dans, le cas des informations statistiques, en dépit du fait que les informations peuvent se présenter sous une forme agrégée, l'échantillon initial peut ne pas être suffisamment important, et que d'autres éléments d'information peuvent permettre d'identifier les personnes concernées.

L'arrêté royal du 13 février 2001 définit les données anonymes comme étant les données qui ne peuvent être mises en relation avec une personne identifiée ou identifiable et qui ne sont donc pas des données à caractère personnel (art. 1er, 5°, de l'arrêté royal du 13 février 2001).

10.1.3.1.1.1.4. La notion de données médicales

Les données médicales sont une catégorie de données à caractère personnel. Elles reçoivent une interprétation large : il s'agit de toute information relative à tout aspect, tant physique que psychique, de la santé, passée, actuelle et future, bonne ou mauvaise, d'une personne physique ([18]).

Cette définition englobe :

- les informations relatives à l'abus d'alcool ou à la consommation de drogues ;
- l'indication du fait qu'une personne s'est blessée au pied et était en congé de maladie partiel, constitue une donnée médicale ([19]) ;
- les données ayant un lien manifeste et étroit avec la santé ;
- les données génétiques dans la mesure où elles donnent une image de la condition physique d'un individu et de son état de santé.

Pour être relative à la santé, la donnée ne doit pas nécessairement émaner d'un professionnel de la santé ou résulter d'un acte réservé aux professionnels de la santé.

Par contre, en principe, est une donnée médicale toute donnée à caractère personnel traitée par un professionnel de la santé à des fins thérapeutiques.

Mais une donnée à caractère personnel peut être relative à la santé même lorsqu'elle n'est pas traitée à des fins thérapeutiques ; c'est le cas notamment en matière d'assurance ou de crédit.

Cependant, la seule information relative à un aspect physique ou psychique d'un individu ne constitue pas en tant que telle une donnée médicale. Pour obtenir cette dernière qualification, l'aspect physique ou psychique doit être *relatif* à la santé de la personne concernée.

10.1.3.1.1.1.5. La personne physique

---

[18] Sur cette notion, voyez : Convention n° 108 précitée, et le considérant n° 45 de son rapport explicatif ; Rec. (97)5 du Conseil de l'Europe du 13 février 1997 sur la protection des données médicales, art. I de l'annexe ; Avis n° 13 du 30 juillet 1999 sur les aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information ; C.J.C.E., 6 novembre 2003, Bodil Lindqvist v. Suède, affaire C-101/01, § 50, obs. C. de TERWANGNE, « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », *R.D.T.I.*, 2004, pp. 67-99 ; Groupe 29, Document de travail sur les données génétiques, WP 91, du 17 mars 2004. Voyez aussi : C.E., arrêt n° 84.800 du 26 janvier 2000 sur le RPM et C.E., arrêt n° 45.218 du 18 décembre 1993 sur le RCM.

[19] C.J.C.E., 6 novembre 2003, Bodil Lindqvist v. Suède, affaire C-101/01, § 51, obs. C. de TERWANGNE, o.c.

Dans le cadre de la loi du 8 décembre 1992, la notion de données à caractère personnel concerne uniquement les personnes physiques vivantes, même si l'on peut regretter cette restriction relative aux personnes décédées ([20]).

Les informations relatives aux personnes morales ne constituent pas des données à caractère personnel.

10.1.3.1.1.2. La notion de traitement

Au sens strict, le traitement est toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel (art. 1er, § 2, de la loi du 8 décembre 1992), telles que :

- la collecte,
- l'enregistrement,
- l'organisation,
- la conservation,
- l'adaptation ou la modification,
- l'extraction, la consultation,
- l'utilisation,
- la communication par transmission, diffusion ou toute autre forme de mise à disposition,
- le rapprochement ou l'interconnexion,
- le verrouillage,
- l'effacement,
- la destruction, etc.

Dans cette perspective, le traitement se conçoit de façon presque « ponctuelle ».

Un traitement peut répondre à différentes finalités d'utilisation.

Mais à la lecture attentive des dispositions de la loi du 8 décembre 1992 en matière de déclaration de traitements, il semble possible de dégager une autre acception à la notion de traitement. En effet, au sens large, elle désigne l'ensemble des opérations qui s'attachent à une même finalité. En ce sens, le traitement se définit par la finalité à laquelle se rattachent ces opérations.

10.1.3.1.1.3. La notion de fichier

---

[20] Sur la question des personnes décédées, voyez : J. HERVEG, « Une vie privée après la mort? Le cas des données relatives au patient », *Journal des tribunaux*, Bruxelles, Larcier, 2005, n° 6189, pp. 489-500.

Le fichier est tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique (art. 1er, § 3, de la loi du 8 décembre 1992).

La directive 95/46/CE précise que le contenu d'un fichier doit être structuré selon des critères déterminés relatifs aux personnes permettant un accès facile aux données à caractère personnel. Mais les dossiers ou les ensembles de dossiers, de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés ne sont pas des fichiers ([21]).

La question du dossier médical « papier » est controversée, mais le courant majoritaire considère qu'il répond généralement aux critères du fichier. Quoiqu'il en soit, la question perd chaque jour un peu plus de son intérêt avec la généralisation de l'informatisation du dossier du patient dans les hôpitaux qui les fait de toute façon tomber dans le champ d'application de la loi du 8 décembre 1992.

10.1.3.1.4. Les traitements exclus du champ d'application de la loi du 8 décembre 1992

La loi du 8 décembre 1992 exclut un certain nombre de traitements de son champ d'application matériel. Il est possible de distinguer à cet égard entre les exclusions totales et les exclusions partielles ([22]).

10.1.3.1.4.1. Les exclusions totales du champ d'application matériel

Les traitements de données à caractère personnel effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques, font l'objet d'une exclusion totale du champ d'application matériel de la loi du 8 décembre 1992.

En présence d'une finalité personnelle ou domestique et d'une autre finalité qui, par nature, n'est pas personnelle ou domestique, tel l'intentement d'une action judiciaire, le traitement tombe sous le coup de la loi du 8 décembre 1992 pour autant que les autres conditions de son application soient réunies.

La Cour de Justice de Luxembourg a précisé que cette exception ne visait que les activités qui s'inséraient dans le cadre de la vie privée ou familiale des particuliers, considérant que ce n'était manifestement pas le cas du traitement de données à caractère personnel consistant

---

21 Considérant 27 de la directive 95/46/CE.

22 A ce sujet, voyez : C. de TERWANGNE, « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », obs. sous C.J.C.E., 6 novembre 2003, Bodil Lindqvist v. Suède, affaire C-101/01, § 50, *R.D.T.I.*, 2004, p. 84 et s.

dans leur publication sur l'Internet de sorte que ces données étaient rendues accessibles à un nombre indéfini de personnes ([23]).

Est-il possible d'en déduire que la restriction de l'accès au site aurait permis une autre réponse ? Il semble en effet possible de soustraire de cette façon les sites Internet qui ne seraient destinés qu'à des finalités exclusivement personnelles ou domestiques, tel le site qui hébergerait des photographies accessibles uniquement aux proches, qu'ils soient de la famille important peu.

Quoiqu'il en soit, la correspondance et la tenue de répertoires au sein d'un hôpital ne bénéficient pas de cette exclusion du champ d'application matériel de la loi du 8 décembre 1992, l'hôpital n'étant de surcroît pas une personne physique.

10.1.3.1.4.2. Les exclusions partielles du champ d'application matériel

L'application de la loi du 8 décembre 1992 est partiellement écartée pour toute une série de traitements de données à caractère personnel qui intéressent la sûreté de l'Etat, la sécurité publique ou encore la lutte contre le blanchiment de capitaux. Il est à noter que le Centre européen pour enfants disparus et sexuellement exploités bénéfice également d'une exemption partielle ([24]).

10.1.3.1.4.3. Le sort des traitements de données exclus du champ d'application de la loi du 8 décembre 1992

La non-application de la loi du 8 décembre 1992 laisse subsister la protection du droit au respect de la vie privée consacrée par l'article 22 de la Constitution et l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Il convient dès lors de procéder dans cette situation au contrôle du respect des exigences que ces dispositions comportent ou induisent au profit de la personne concernée.

10.1.3.1.2. Champ d'application territorial de la loi du 8 décembre 1992

10.1.3.1.2.1. Etablissement fixe en Belgique

La loi du 8 décembre 1992 s'applique au traitement de données à caractère personnel effectué dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement sur le territoire belge (art. 3 bis, al. 1, 1°, loi du 8 décembre 1992).

La directive 95/46/CE précise que l'établissement sur le territoire d'un Etat membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable. De plus, la forme

---

[23] C.J.C.E., 6 novembre 2003, Bodil Lindqvist v. Suède, affaire C-101/01, § 47, obs. C. de TERWANGNE, o.c.

[24] Voyez à ce sujet les §§ 3 à 6 de l'article 3 de la loi du 8 décembre 1992.

juridique retenue pour cet établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard ([25])

Le Groupe 29 nous apprend que le lieu d'établissement d'un responsable de traitement implique l'exercice effectif et réel d'une activité au travers d'accords stables et doit être déterminé conformément à la jurisprudence de la Cour de justice européenne, ce qui implique l'exercice réel d'une activité dans un lieu d'établissement fixe pour une période indéterminée. L'exigence est également remplie si la société est constituée pour une période donnée. Il donne l'exemple du lieu d'établissement d'une société qui fournit des services par le biais d'un site Internet. Il ne s'agit pas du lieu où est située la technologie qui supporte son site web ni le lieu d'accès au site web mais le lieu où la société exerce son activité ([26]).

Les hôpitaux belges répondent, bien entendu, à ces conditions.

De plus, ayant en vue les « fusions-acquisitions » en matière hospitalière au sein de l'Union européenne, il paraît opportun de rappeler que, lorsqu'un même responsable est établi sur le territoire de plusieurs Etats membres, en particulier par le biais d'une filiale, il doit s'assurer, notamment, en vue d'éviter tout contournement, que chacun des établissements remplit les obligations prévues par le droit national applicable aux activités de chacun d'eux ([27]).

10.1.3.1.2.2. Recours à des moyens situés en Belgique

La loi du 8 décembre 1992 s'applique lorsque le responsable du traitement n'est pas établi de manière permanente sur le territoire de la Communauté européenne mais qu'il recourt, à des fins de traitement de données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire belge, autres que ceux qui sont exclusivement utilisés à des fins de transit sur le territoire belge (art. 3 bis, al. 1, 2°, loi du 8 décembre 1992).

Dans ce cas, le responsable du traitement doit désigner un représentant établi sur le territoire belge, sans préjudice des actions qui pourraient être introduites contre le responsable du traitement lui-même (art. 3 bis, al. 2, loi du 8 décembre 1992).

10.1.3.2. Identification des acteurs des traitements de données à caractère personnel

Le respect de la loi du 8 décembre 1992 implique d'identifier les acteurs qui sont susceptibles d'intervenir dans sa mise en œuvre.

---

[25] Considérant n° 19 de la directive 95/46/CE.

[26] Document de travail : application internationale du droit de l'UE en matière de protection des données au traitement de données à caractère personnel sur Internet par des sites web établis en dehors de l'UE, adopté le 30 mai 2002, WP 56.

[27] Considérant n° 19 de la directive 95/46/CE.

10.1.3.2.1. La personne concernée

La personne concernée s'identifie conformément aux critères qui ont été dégagés pour déterminer la présence d'une donnée à caractère personnel : il s'agit de la personne concernée par l'information faisant l'objet d'un traitement.

A lire le rapport explicatif de la Convention n° 108 du Conseil de l'Europe, cette notion exprime l'idée selon laquelle toute personne possède un droit subjectif par rapport aux informations qui la concernent, même si ces informations sont rassemblées par d'autres ([28]). Le sens à donner à cette explication est ambigu.

En tout cas, au sein de l'hôpital, il existe déjà deux grandes catégories de personnes concernées : les patients et les membres du personnel, même si nous ne nous intéressons présentement qu'aux premiers ([29]).

10.1.3.2.2. Le responsable du traitement

Le responsable du traitement est tenu d'assurer la majeure partie des obligations imposées par la loi du 8 décembre 1992. Il doit veiller au respect des conditions générales de licéité du traitement de données à caractère personnel, fournir un certain nombre d'informations à la personne concernée, assurer la confidentialité et la sécurité du traitement, et déclarer le traitement auprès de la Commission de protection de la vie privée.

Concrètement, il s'agit de la personne (que ce soit une personne physique ou morale, une association de fait ou une administration publique importe peu) qui, seule ou conjointement avec d'autres, détermine les **finalités** et les **moyens** du traitement de données à caractère personnel. Elle est la personne qui a la maîtrise sur ces deux éléments de la définition ; elle est la personne qui décide des finalités du traitement des données du patient (dossier informatisé du patient, facturation, recouvrement, etc.) et qui décide des moyens financiers, matériels et humains à mettre en œuvre pour atteindre ces finalités. Il faut également insister sur le fait qu'il peut y avoir plusieurs responsables de traitement ; ce seront des coresponsables ([30]).

L'identification du responsable du traitement dépend d'une analyse au cas par cas, sauf lorsqu'il est désigné par ou en vertu de la loi, du décret ou de l'ordonnance qui détermine les finalités et les moyens du traitement (art. 1er, § 4, de la loi du 8 décembre 1992).

---

28 Convention n° 108, Rapport explicatif, n° 28.

29 S'agissant des membres du personnel, il est utile de rappeler les conventions collectives du travail n° 68 conclue le 16 juin 1998 au sein du Conseil national du Travail, relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail, et n° 81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau.

30 **J.-M. VAN GYSEGHEM, « Les modifications de la relation médecin-patient au contact de la télématique médicale : quelques réflexions à bâtons rompus », *Lex Electronica*, vol. 10, n° 3, 2006.**

Le nom du responsable du traitement doit être indiqué dans la déclaration de traitement à adresser à la Commission pour la Protection de la Vie Privée (art. 17, § 3, 2°, de la loi du 8 décembre 1992), ainsi que dans le règlement de l'hôpital relatif à la protection de la vie privée (qui doit être remis à chaque patient) ([31]).

Cependant, au sein d'un hôpital, l'identification du responsable du traitement n'est pas toujours une chose aisée ([32]).

Qui peut ou doit se voir reconnaître la qualité de responsable du traitement de données ? La personne morale qui exploite l'hôpital ? Le gestionnaire de l'hôpital ? Le directeur administratif ? Le directeur médical ? Le médecin-chef ? Le chef du département infirmier ? Chaque chef de service ou de département ? Chaque praticien professionnel en ce qui concerne ses activités ? Faut-il distinguer en outre selon le statut de salarié ou d'indépendant du personnel ?

La loi relative aux hôpitaux ne contient pas de disposition spécifique relative à la détermination du responsable du traitement de données. De manière générale, elle pose que *la responsabilité générale et finale pour l'activité hospitalière, sur le plan de l'organisation et du fonctionnement, ainsi que sur le plan financier, incombe au gestionnaire* de l'hôpital ([33]). Ce dernier a aussi la charge de définir *la politique générale de l'hôpital* (~~)~~et de prendre *les décisions de gestion en respectant les dispositions et procédures spécifiques prévues au titre IV* de la loi ([34]).

La loi relative aux hôpitaux instaure aussi diverses responsabilités quant à l'organisation de l'activité médicale et infirmière à charge du médecin-chef et du chef du département infirmier notamment en ce qui concerne l'ouverture et la conservation du dossier du patient ([35]).

---

[31] Arrêté royal du 23 octobre 1964 portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre (annexe, III, Normes d'organisation, 9° quater). Cet arrêté n'a pas cependant pas été mis à jour suite à la transposition de la directive 95/46/CE. Il correspond à une recommandation du Conseil de l'Europe (Rec. n° (97) 5, art. 9.3).

[32] Sur cette question, voyez : J. HERVEG, M.-N. VERHAEGEN et Y. POULLET, « Les droits du patient face au traitement informatisé de ses données dans une finalité thérapeutique : les conditions d'une alliance entre informatique, vie privée et santé », *Rev. dr. Santé*, 2002-2003/2, pp. 56-84, spéc. n° 13.

[33] **Art. 16, al. 1er, de la loi relative aux hôpitaux. Le gestionnaire est *l'organe qui, selon le statut juridique de l'hôpital, est chargé de la gestion de l'exploitation de l'hôpital* » (art. 8, 1°, de la même loi).**

[34] **Art. 16, al. 2, de la loi relative aux hôpitaux.**

[35] **Art. 18, 19, 20, 21, 23, 24, 25, et 26 de la loi relative aux hôpitaux**. Voir aussi les dispositions spécifiques relatives au dossier médical ou infirmier en fonction du service hospitalier considéré, contenues dans l'arrêté royal du 23 octobre 1964, ainsi que les arrêtés royaux du 15 décembre 1987 portant exécution des articles 13 à 17 de la loi relative aux hôpitaux, coordonnée le 7 août 1987, du 3 mai 1999 déterminant les conditions générales minimales auxquelles le dossier médical, visé à l'article 15 de la loi relative aux hôpitaux, coordonnée le 7 août 1987, doit répondre, et

Mais cela n'implique pas nécessairement que ces personnes sont celles qui, dans les faits, déterminent les finalités et les moyens du traitement de données. La notion de responsable est en effet ambiguë : elle désigne tant la personne qui dans les faits détermine les finalités et les moyens du traitement de données, que la personne ou l'organe qui selon ses compétences aurait pu et du définir ces finalités et ces moyens. L'exposé des motifs précise à cet égard que *« L'important est que le responsable du traitement soit la personne, l'instance administrative, la société, l'association, etc. qui dispose du pouvoir de décision sur le traitement effectué. »* ([36])

Il semble que, à ce jour, la meilleure réponse consiste à partir du fait que le responsable du traitement de données devrait être la personne morale qui exploite l'hôpital, et que le gestionnaire assume la responsabilité générale et finale de cette exploitation. Il va de soi que la personne morale exercera ses droits et obligations au travers des différents organes par lesquels elle agit, conformément à la loi ou à ses statuts, sans préjudice des représentations conventionnelles ou ratifications éventuelles. En tout état de cause, lorsqu'une personne de l'hôpital signe le formulaire de déclaration de traitement à la Commission de protection de la vie privée, il devrait être clair qu'elle signe *qualita quae*, c'est-à-dire eu égard à sa fonction au sein de l'hôpital et non en nom personnel. Autrement dit, c'est l'hôpital qu'elle engage ce faisant, et non sa personne.

Mais il faut insister sur le fait que si une personne détermine les finalités et les moyens d'un traitement de données à caractère personnel au sein de l'hôpital, sans respecter les règles de répartition des fonctions en la matière au sein de l'hôpital, elle aura la qualité de responsable de traitement pour les traitements qu'elle aura initiés. La seule différence avec l'hypothèse précédente c'est que, dans ce dernier cas, la licéité du traitement pourrait être mise en cause et que la personne pourrait devoir répondre du non-respect des règles de fonctionnement de l'hôpital. L'exemple-type est le chef de service qui informatise le dossier médical hospitalier des patients de son service, de façon autonome au sein de l'hôpital (tant pour la détermination des finalités que des moyens), c'est-à-dire sans s'inscrire dans l'organisation générale de l'hôpital notamment en termes de gestion informatique.

10.1.3.2.3. La personne, placée sous l'autorité directe du responsable du traitement, habilitée à traiter les données

La loi du 8 décembre 1992 distingue la notion de personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données. La notion d'autorité directe ne s'entend pas ici au sens classique du droit du travail. C'est un concept qui doit recevoir une interprétation autonome.

---

du 28 décembre 2006 déterminant les conditions générales minimales auxquelles le dossier infirmier, visé à l'article 17*quater* de la loi relative aux hôpitaux, coordonnée le 7 août 1987, doit répondre.

[36] Doc. Parl., Ch. *s.o.*, 1998-1999, n°1566/1, p.15

Au sein de l'hôpital, cette notion vise l'ensemble des personnes qui sont soumises à l'autorité directe de l'hôpital. Concrètement, il s'agit du personnel médical, salarié ou indépendant, du personnel infirmier, para-médical, administratif et technique (en ce compris le service informatique), etc.

Par contre, la société extérieure en charge de la maintenance informatique n'est pas, en principe, sous l'autorité directe de l'hôpital. Il faut aussi vérifier dans quelle mesure elle doit recevoir la qualité de « sous-traitant » de données à caractère personnel pour compte de l'hôpital.

10.1.3.2.4. Le professionnel des soins de santé sous la responsabilité duquel le traitement de données médicales doit être effectué

La loi du 8 décembre 1992 indique que le traitement de données médicales ne peut être effectué que sous la **responsabilité** d'un professionnel des soins de santé, sauf dans le cas d'un consentement écrit de la personne concernée ou lorsque le traitement est nécessaire pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée (art. 7, § 4, al. 1, de la loi du 8 décembre 1992).

Le contenu de cette fonction de « responsabilité » n'est pas défini par la loi.

En tout cas, cette responsabilité, que l'on peut penser être « organisationnelle » (ce qui fait penser au médecin-chef pour l'ouverture et la conservation du dossier médical hospitalier du patient) ne se confond pas nécessairement avec celle du responsable du traitement. Il s'agit de deux fonctions distinctes, même si elles peuvent être exercées par une seule et même personne.

10.1.3.2.5. Le professionnel des soins de santé sous la surveillance duquel le traitement de données médicales doit être effectué

La loi du 8 décembre 1992 précise que le traitement de données médicales à fins thérapeutiques (art. 7, § 2, j, de la loi du 8 décembre 1992) doit se faire sous la **surveillance** d'un professionnel des soins de santé, sans en préciser non plus le contenu.

Cette « surveillance » semble renvoyer à une fonction qui consisterait à exercer une supervision, un contrôle, sur le traitement de données en tant que tel. Ce contrôle induit le pouvoir de s'assurer des habilitations dans le traitement des données, ce qui constitue une mesure de sécurité supplémentaire.

En règle, le surveillant ne peut être que le praticien en charge de la personne concernée par le traitement de données médicales.

En tout cas, ici aussi, cette fonction ne doit pas obligatoirement être prise en charge par le responsable du traitement ou par le professionnel des soins de santé sous la responsabilité duquel le traitement de données médicales doit être effectué.

Il s'ensuit que nous serions en présence de trois fonctions distinctes qui, au sein de l'hôpital, pourraient, en fonction des circonstances, être exercées par une, deux voire trois personnes différentes. A cet égard, il ne semble pas opportun de hiérarchiser ces trois fonctions. Par contre, il convient de les articuler avec discernement. C'est ainsi que l'hôpital, en tant que tel, n'a pas la compétence pour exercer les fonctions de responsabilité et de surveillance sous lesquelles le traitement de données médicales doit être effectué, à défaut d'être un professionnel des soins de santé au sens strict (cf. *infra* sur cette notion). Inversement, les professionnels des soins de santé qui exerceraient ces deux fonctions n'ont pas nécessairement la compétence pour endosser la fonction de responsable de traitement.

10.1.3.2.6. Le professionnel des soins de santé sous la responsabilité et la surveillance duquel le traitement de données médicales doit être effectué

L'arrêté royal du 23 octobre 1964, non-modifié sur ce point suite à la transposition de la directive 95/46/CE, prévoit toujours que le « maître du fichier » doit désigner le médecin qui exerce la responsabilité et la surveillance sous lesquelles les « données médicales à caractère personnel » devaient être traitées sous l'empire de la version précédente de la loi du 8 décembre 1992.

Si l'on admet que le responsable du traitement remplace la fonction de maître de fichier, ce qui pourrait cependant être contesté, cela signifierait qu'il lui incomberait de désigner au sein de l'hôpital un médecin en charge de ces deux fonctions reprises *mutatis mutandis* dans la nouvelle mouture de la loi du 8 décembre 1992. En réalité, le responsable du traitement ne devrait désigner que le professionnel des soins de santé sous la responsabilité duquel le traitement de données médicales doit être effectué, par exemple le médecin-chef pour l'ouverture et la conservation du dossier médical hospitalier du patient, étant entendu qu'il n'est pas possible, sous la mouture actuelle de la loi du 8 décembre 1992, de désigner, au sens littéral du terme, dans chaque cas d'espèce, le professionnel des soins de santé sous la surveillance duquel le traitement de données médicales doit être effectué.

10.1.3.2.7. La notion de professionnel des soins de santé

A ce jour, le Roi n'a pas encore déterminé les catégories de personnes qui pouvaient être considérées comme des professionnels des soins de santé.

L'exposé des motifs de la loi du 8 décembre 1992, dans sa version initiale, expliquait que le « professionnel des soins de santé » (remplaçant la notion de « praticien de l'art de guérir ») et seul apte à occuper les *fonctions de responsabilité et de surveillance* des données médicales, correspond à un vaste concept qui fait référence à l'ensemble des personnes qui *prestent* des

soins de santé à l'égard d'autres personnes dans l'exercice de leur profession. Cette notion se rapproche de celle de « praticien professionnel » visée dans la loi relative aux droits du patient ([37]).

10.1.3.2.8. Le préposé à la protection des données

La loi du 8 décembre 1992 prévoit que le Roi peut déterminer que le responsable du traitement désigne un *préposé à la protection des données* chargé d'assurer, d'une manière indépendante, l'application de loi ainsi que de ses mesures d'exécution (art. 17 bis de la loi du 8 décembre 1992) ([38]).

Cette fonction n'a pas été imposée en milieu hospitalier et cela peut être regretté.

10.1.3.2.9. Le conseiller en sécurité en milieu hospitalier

L'arrêté royal du 23 octobre 1964, également non-modifié sur ce point suite à la transposition de la directive 95/46/CE, prévoit que le « maître du fichier » doit désigner un conseiller en sécurité ([39]).

Il prévoit que la mission de ce conseiller en sécurité est de conseiller le « responsable de la gestion journalière » au sujet de tous les aspects de la sécurité de l'information.

Sur la distinction entre le conseiller en sécurité et le préposé à la protection des données, la Commission de protection de la vie prive nous apprend que ([40]) :

> « *(…) le conseiller en sécurité doit effectivement veiller à la sécurité des applications et à la prise des mesures techniques et organisationnelles appropriées de manière à garantir le respect de la confidentialité des données et veiller aux contrôles d'accès et autres. (…) Par ailleurs, la nécessité de veiller lors de chaque traitement au respect d'autres principes de la loi de 1992 comme celui de la proportionnalité, celui de l'accès etc. rend nécessaire l'accomplissement d'une autre fonction : celle de « préposé à la protection des données », notion différente utilisée par la LVP (article 17 bis), notion qui couvre d'autres compétences que celle de veiller à la seule sécurité des données mais comprend également le devoir de « s'assurer de manière indépendante l'application de la présente loi ainsi que de ses mesures d'exécution »,*

---

[37] Sur ceci, voyez : J. HERVEG, M.-N. VERHAEGEN et Y. POULLET, o.c., n° 14 ; Y. POULLET, « Construire un cadre juridique pour l'e-Health », in J. HERVEG (éd.), La protection des données médicales – Les défis du XXIe siècle. The Protection of Medical Data – Challenges of the 21st Century, Louvain-la-Neuve, Anthémis, Paris, L.G.D.J., 2008, p. 99, n° 9.

[38] Sur cette notion, voyez l'avis n° 33/2002 du 22 août 2002 de la Commission de protection de la vie privée à propos du Centre fédéral d'expertise des soins de santé, p. 11, n° 21.

[39] Arrêté royal du 23 octobre 1964, annexe, N 1, annexe A, III, normes d'organisation, 9 quater, g.

[40] Avis n° 33/2002 du 22 août 2002 précité.

ce qui signifie outre le contrôle du caractère adéquat des mesures de sécurité, celle du contrôle du respect des principes de légitimité, de proportionnalité et du droit d'accès des personnes concernées. La Commission si elle estime fondée la distinction des deux fonctions, ne s'oppose pas cependant pas au fait que ce soit une seule et même personne qui cumule les deux fonctions et joue le rôle de contrôleur interne, étant entendu que la loi garantira à cette personne, l'indépendance indispensable à l'achèvement de cette double tâche et surtout mettra en place la commission sectorielle d'autorisation que la Commission réclame et qui jouera le rôle de contrôleur externe (…) ».

Le conseiller en sécurité ne se confond dès lors pas avec le préposé à la protection des données.

10.1.3.2.10. Le sous-traitant

Le sous-traitant est la personne physique ou morale, l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données (art. 1, § 5, de la loi du 8 décembre 1992) ([41]).

S'il faut bien sûr penser aux sociétés extérieures en charge du développement et de la maintenance des systèmes informatiques, il est aussi possible de se pencher sur le cas des analyses médicales confiées à des laboratoires extérieurs. En effet, dans le cas d'une analyse sanguine confiée à un tel laboratoire, s'il est acquis que le sang n'est pas une donnée à caractère personnel, le fait de l'analyser est une opération qui consiste à extraire de l'information concernant une personne physique identifiée ou identifiable, en tout cas dans le cadre des activités normales d'un hôpital. De ce fait, il s'agit d'un traitement de données à caractère personnel qui tombe sous le coup de la loi du 8 décembre 1992, prenant en considération le recours à des moyens automatisés. Mais la particularité qui nous intéresse présentement réside dans le fait que l'hôpital a confié la réalisation de cette opération à un laboratoire qui lui est extérieur ou, pour être plus précis, qui n'est pas placé sous son autorité directe. *A contrario*, il ne s'agit pas de sous-traitance lorsque l'analyse est confiée au laboratoire de l'hôpital qui est soumis à son autorité directe.

Cette qualification emporte des conséquences notables notamment en termes de convention écrite entre les parties, de détermination des mesures visant à assurer la confidentialité et la sécurité du traitement de données à caractère personnel, et de répartition des responsabilités (cf. *infra*, la confidentialité et la sécurité des traitements de données à caractère personnel).

10.1.3.2.11. Tiers

[41] **Voyez not. : J. HERVEG et J.-M. VAN GYSEGHEM, « La sous-traitance des données du patient au regard de la directive 95/46/CE », *Lex Electronica*, vol. 9, n° 3, 2004.**

Le tiers est la personne physique, la personne morale, l'association de fait ou l'administration publique, autre que (art. 1, § 6, de la loi du 8 décembre 1992) :

- la personne concernée,
- le responsable du traitement,
- le sous-traitant,
- et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données.

10.1.3.2.12. Destinataire

Le destinataire est la personne physique, la personne morale, l'association de fait ou l'administration publique qui reçoit communication de données, qu'il s'agisse ou non d'un tiers (art. 1, § 7, de la loi du 8 décembre 1992). Cela peut donc être aussi bien le patient qu'une personne en charge de ce dernier ou un membre du personnel administratif.

La loi précise que les instances administratives ou judiciaires qui sont susceptibles de recevoir communication de données dans le cadre d'une enquête particulière ne sont toutefois pas considérées comme des destinataires (art. 1, § 7, de la loi du 8 décembre 1992).

10.1.3.2.13. Organisation intermédiaire

L'organisation intermédiaire est la personne physique ou morale, l'association de fait ou l'administration publique, autre que le responsable du traitement des données non-codées, qui code les données (art. 1er, 6°, de l'arrêté royal du 13 février 2001). Cette organisation intervient dans le cadre des traitements ultérieurs de données à caractère personnel à des fins historiques, statistiques ou scientifiques.

10.1.3.3. Conditions générales de licéité des traitements de données à caractère personnel

Les traitements de données à caractère personnel sont soumis à des conditions générales de licéité qui peuvent être regroupées sous la bannière de trois principes fondamentaux :

- Le principe de finalité ;
- Les principes de loyauté et de licéité ;
- Le principe de qualité des données.

Cette classification ou catégorisation n'enlève rien au fait que les dispositions de la loi du 8 décembre 1992 se lisent simultanément ou, pour être plus précis, le respect de l'une s'apprécie au regard de celui des autres.

Le non-respect des conditions générales de licéité est passible d'une amende de 100 à 100.000 EUR (+ application des décimes additionnels)

10.1.3.3.1. Le principe de finalité : déterminée, explicite et légitime

Le principe de finalité est la pierre angulaire de la loi du 8 décembre 1992 ([42]). Il signifie qu'il faut, avant toute chose, distinguer la raison d'être de l'opération à intervenir sur les données à caractère personnel. C'est à partir de cette raison, de cette finalité, que l'ensemble de réglementation des traitements de données à caractère personnel va pouvoir être adéquatement appliqué. Nous l'avons déjà vu, au sein d'un hôpital, les raisons de traiter des données à caractère personnel concernant les patients sont nombreuses ; de la constitution et de la gestion de leurs dossiers, à la facturation des prestations hospitalières en n'omettant pas les exigences en terme de santé publique et de financement des soins de santé. Il est aussi opportun de songer à une finalité qui consiste à pouvoir se défendre en cas de mise en cause de sa responsabilité, de demande d'indemnisation ou pour recouvrer les montants dus ([43]).

La loi du 8 décembre 1992 impose que les données à caractère personnel soient collectées pour des finalités déterminées, explicites et légitimes (art. 4, § 1er, 1°, de la loi du 8 décembre 1992).

L'exigence de **détermination** signifie que la finalité pour laquelle les données à caractère personnel sont collectées doit être adéquatement circonscrite dans son contenu ; son étendue doit être fixée. A cet égard, plus la donnée est sensible, plus la finalité doit être précisément

---

42 Th. LEONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, p. 384, n° 24 et les références indiquées à la note infra-paginale n° 77.

43 Il convient aussi d'envisager les obligations relatives à la traçabilité du sang imposées par l'arrêté royal du 23 octobre 1964 et par l'arrêté royal du 17 février 2005 fixant les normes auxquelles une banque de sang hospitalière doit répondre pour être agréée.

déterminée. Ainsi, collecter des données à des fins de recherche scientifique ne semble pas suffisant au regard de l'exigence de détermination. Il convient de préciser la nature du projet, ses objectifs, et le nom de la personne ou de l'organisme pour le compte duquel la recherche est effectuée ([44]).

Le caractère **explicite** de la finalité requiert qu'elle soit énoncée et non seulement sous-entendue ou implicite.

Le caractère **légitime** de la finalité implique qu'elle respect l'équilibre entre les intérêts en présence, les exigences étant d'autant plus fortes en présence de données « sensibles ». La loi du 8 décembre 1992 distingue d'ailleurs entre les données « normales » et les données « sensibles ». Le caractère légitime implique l'obligation d'opter pour les moyens les moins attentatoires aux intérêts, droits et libertés de la personne concernée.

La loi du 8 décembre 1992 fournit les hypothèses dans lesquelles la légitimité de la finalité du traitement de données à caractère personnel « normales » est présumée (art. 5 de la loi du 8 décembre 1992), ce qui implique de la vérifier concrètement dans chaque cas d'espèce. Elle précise d'ailleurs que le traitement de données à caractère personnel ne peut être effectué que dans l'une de ces hypothèses. Celles-ci sont les suivantes :

a) lorsque la personne concernée a indubitablement donné son consentement ([45]) ;
b) lorsqu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
c) lorsqu'il est nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance ;
d) lorsqu'il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ;
e) lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ;
f) lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui peut prétendre à une protection au titre de la présente loi.

   La loi précise que le Roi peut, par arrêté délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée, préciser les cas où la condition mentionnée sous f) est considérée ne pas être remplie.

---

[44] Voyez à ce propos : Conseil de l'Europe, Rec. N° R (83) 10 relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques, art. 3.1.

[45] Pour rappel, le consentement est toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement (art. 1, § 8, de la loi du 8 décembre 1992).

Ensuite, conformément à la directive 95/46/CE, la loi du 8 décembre 1992 **interdit** le traitement des données sensibles, ce qui inclut notamment les données médicales, tout en prévoyant une série de cas dans lesquels cette interdiction ne s'applique pas (voyez les art. 6, 7 et 8, de la loi du 8 décembre 1992). En ce qui concerne les données médicales, l'interdiction ne s'applique pas dans les cas suivants (art. 7 de la loi du 8 décembre 1992) :

a) lorsque la personne concernée a donné son consentement **par écrit** à un tel traitement, pour autant que ce consentement puisse à tout moment être retiré par celle-ci ;
b) lorsque le traitement est nécessaire afin d'exécuter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail ;
c) lorsque le traitement est nécessaire à la réalisation d'une finalité fixée par ou en vertu de la loi, en vue de l'application de la sécurité sociale ;
d) lorsque le traitement est nécessaire à la promotion et à la protection de la santé publique y compris le dépistage ;
e) lorsque le traitement est rendu obligatoire par ou en vertu d'une loi, d'un décret ou d'une ordonnance pour des motifs d'intérêt public importants ;
f) lorsque le traitement est nécessaire à la défense des intérêts vitaux ([46]) de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
g) lorsque le traitement est nécessaire pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée ;
h) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée ;
i) lorsque le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
j) lorsque le traitement est nécessaire aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée et les données sont traitées sous la surveillance d'un professionnel des soins de santé ;
k) lorsque le traitement est nécessaire à la recherche scientifique et est effectué conformément aux conditions fixées par l'arrêté royal du 13 février 2001.

Le Roi a requis du responsable du traitement qu'il prenne des mesures supplémentaires lors du traitement de données sensibles (art. 25 à 27 de l'arrêté royal du 13 février 2001), ce qui donne les obligations suivantes en ce qui concerne les données médicales :

---

[46] La notion d'intérêt vital vise expressément et exclusivement la situation de péril imminent à la vie d'une personne physique, qu'il s'agisse de la personne concernée ou de toute autre personne physique. Il ne peut pas en être déduit que la personne concernée, capable physique et juridiquement de consentir, pourrait, sans autre forme de procès, refuser d'autoriser le traitement de ses données médicales lorsque les intérêts vitaux d'une autre personne sont en jeu. Il conviendrait alors d'examiner la qualification à donner à ce comportement au regard des normes applicables.

1° les catégories de personnes ayant accès aux données à caractère personnel doivent être désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées ;
2° la liste des catégories des personnes ainsi désignées doit être tenue à la disposition de la Commission par le responsable du traitement ou, le cas échéant, par le sous-traitant ;
3° le responsable du traitement doit veiller à ce que les personnes ainsi désignées soient tenues par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données médicales ;
4° lorsque l'information relative au traitement de données à caractère personnel est communiquée à la personne concernée ou lors de la déclaration du traitement à la Commission de protection de la vie privée, le responsable du traitement doit mentionner la base légale ou réglementaire autorisant le traitement de données médicales.

Lorsque le traitement de données médicales est exclusivement autorisé par le consentement par écrit de la personne concernée, le responsable du traitement doit préalablement communiquer à la personne concernée, en sus des informations dues en vertu de l'article 9 de la loi, les motifs pour lesquelles ces données sont traitées ainsi que la liste des catégories de personnes ayant accès aux données à caractère personnel (art. 26 de l'arrêté royal du 13 février 2001).

Lorsque le traitement de données médicales est exclusivement autorisé par le consentement écrit de la personne concernée, ce traitement est néanmoins interdit lorsque le responsable du traitement est l'employeur présent ou potentiel de la personne concernée ou lorsque la personne concernée se trouve dans une situation de dépendance vis-à-vis du responsable du traitement, qui l'empêche de refuser librement son consentement. Cette interdiction est levée lorsque le traitement vise l'octroi d'un avantage à la personne concernée (art. 27 de l'arrêté royal du 13 février 2001).

De manière générale, il faut rappeler que, sauf dans le cas d'un consentement écrit de la personne concernée ou lorsque le traitement est nécessaire pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée, le traitement des données à caractère personnel relatives à la santé ne peut être effectué que sous la responsabilité d'un professionnel des soins de santé (art. 7, § 4, de la loi du 8 décembre 1992).

La loi précise que, lors d'un traitement de données médicales, ce professionnel des soins de santé et ses préposés ou mandataires sont soumis au secret (art. 7, § 4, de la loi du 8 décembre 1992). Ce secret n'est pas nécessairement celui visé à l'article 458 du Code pénal.

Enfin, la loi ajoute que les données médicales doivent être collectées auprès de la personne concernée et qu'elles ne peuvent être collectées auprès d'autres sources qu'à condition que la collecte soit (art. 7, § 5, de la loi du 8 décembre 1992) :

- conforme aux dispositions particulières fixées aux articles 25 à 27 de l'arrêté royal du 13 février 2001 visées ci-avant (catégories de personnes ayant accès aux données, respect du caractère confidentiel des données, indication de la base légale ou réglementaire autorisant le traitement des données, informations complémentaires à la personne concernée, relation de travail),
- réalisée sous la responsabilité d'un professionnel des soins de santé soumis ainsi que ses préposés ou mandataires au secret,
- et qu'elle soit nécessaire aux fins du traitement ou que la personne concernée ne soit pas en mesure de fournir les données elle-même.

Le principe de finalité induit une autre conséquence qui est relative à la compatibilité des opérations sur les données à caractère personnel au regard de la finalité poursuivie. En effet, la loi du 8 décembre 1992 précise que les données à caractère personnel ne peuvent pas être traitées ultérieurement de manière incompatible avec les finalités pour lesquelles elles ont été collectées. Ceci signifie que les opérations dont la réalisation est envisagée sur les données à caractère personnel doivent être compatibles avec la finalité pour laquelle ces données ont été collectées. Si ces opérations ne sont pas compatibles, elles sont interdites (art. 4, § 1er, 2°, de la loi du 8 décembre 1992), ce qui implique de recommencer toute la procédure si leur traitement est toujours envisagé.

Pour apprécier le caractère compatible des traitements ultérieurs avec les finalités pour lesquelles les données ont été collectées, la loi du 8 décembre 1992 indique qu'il faut tenir compte de tous les facteurs pertinents, ce qui comprend notamment (art. 4, § 1er, 2°, de la loi du 8 décembre 1992) :

- les prévisions raisonnables de la personne concernée,
- ainsi que les dispositions légales et réglementaires applicables.

Il faut donc tenir compte des particularités de chaque cas d'espèce. Ainsi, ~~**la loi relative aux hôpitaux impose que**~~ les hôpitaux universitaires ~~**soient**~~ **doivent être** actifs dans le domaine de la recherche clinique, du développement et de l'évaluation de nouvelles technologies médicales ainsi que dans le domaine de l'évaluation d'activités médicales ([47]). Par voie de conséquence, sauf circonstances particulières, il ne semble pas déraisonnable de considérer que, dans un hôpital universitaire, l'utilisation ultérieure des données du patient à des fins de recherche clinique, de développement et d'évaluation de nouvelles technologies médicales ou d'activités médicales, soit compatible avec la finalité thérapeutique pour laquelle elles ont été initialement collectées, ce qui n'exempt pas du respect du reste de la loi du 8 décembre 1992. Par ailleurs, il convient aussi de se référer aux obligations légales en matière d'enregistrement médical.

---

[47] Art. 1er, 7°, de l'arrêté royal du 7 juin 2004 fixant les conditions de désignation en qualité d'hôpital universitaire, de service hospitalier universitaire, fonction hospitalière universitaire ou programme de soins hospitalier universitaire.

En tout état de cause, un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible lorsqu'il respecte les conditions posées par l'arrêté royal du 13 février 2001 (voyez spécialement son chapitre II). Autrement dit, le respect de ces conditions permet de traiter ultérieurement des données à caractère personnel à des fins historiques, statistiques ou scientifiques ([48]).

En tout état de cause aussi, il n'est pas inutile de rappeler que l'opération qui consiste à rendre anonymes des données à caractère personnel paraît devoir être toujours considérée comme étant compatible. En effet, cette opération a pour effet d'offrir la meilleure protection à la personne concernée. D'ailleurs, le responsable du traitement a l'obligation de s'assurer que les données ne soient pas conservées sous une forme permettant l'identification de la personne concernée au-delà de ce qui est nécessaire pour réaliser la finalité pour lesquelles elles ont été collectées ou pour lesquelles elles seront traitées ultérieurement.

Il va de soi que cette opération d'anonymisation ne peut s'envisager que si elle ne contrarie pas une obligation légale ou réglementaire de conserver les données à caractère personnel en cause. Ainsi, par exemple, l'hôpital, par le biais du médecin-chef, a l'obligation de conserver le dossier médical hospitalier des patients pendant une période de trente ans dans l'hôpital ([49]). L'hôpital peut rendre anonyme les données médicales du patient pour les utiliser à des fins scientifiques. Par contre, il ne peut pas, durant cette période de trente ans, rendre anonyme le contenu du dossier médical hospitalier.

Une fois que les données à caractère personnel sont rendues anonymes, elles sortent du champ d'application de la loi du 8 décembre 1992.

10.1.3.3.2. Les principes de loyauté et de licéité

Le principe de loyauté requiert de respecter la finalité qui a été annoncée pour justifier la collecte des données à caractère personnel. Ce principe renvoie à l'exigence de transparence du traitement des données à caractère personnel assuré par les obligations d'information de la personne concernée et de notification du traitement à la Commission de protection de la vie privée (art. 4, § 1er, 1°, de la loi du 8 décembre 1992).

Le principe de licéité requiert le respect des conditions qui sont propres aux données traitées. L'exemple type est celui du respect des règles relatives au secret médical ou celles relatives à la tenue des dossiers médicaux et infirmiers hospitaliers. Le traitement des données du patient doit se faire dans le respect de ces règles pour être licite.

---

[48] Le traitement ultérieur de données à caractère personnel à des fins statistiques, historiques et scientifiques ne sera pas envisagé dans la présente contribution.

[49] Art. 1, § 3, de l'arrêté royal du 3 mai 1999 déterminant les conditions générales auxquelles le dossier médical, visé à l'article 15 **(maintenant 20**) de la loi sur les hôpitaux, coordonnée le 7 août 1987, doit répondre.

10.1.3.3.3. Le principe de qualité des données

Le principe de qualité des données emporte plusieurs conséquences distinctes.

D'abord, les données à caractère personnel doivent être **adéquates, pertinentes et non excessives** au regard des finalités pour lesquelles elles ont été obtenues et pour lesquelles elles sont traitées ultérieurement (art. 4, § 1er, 3°, de la loi du 8 décembre 1992). Le principe de finalité démontre à nouveau son importance dès lors que la finalité poursuivie par le traitement de données est le référent qui permet d'apprécier cette dimension du principe de qualité.

En matière de dossiers hospitaliers, l'hôpital doit notamment se référer à :

- l'arrêté royal du 15 décembre 1987 portant exécution des articles 13 à 17 **(maintenant 18 à 22)** de la loi sur les hôpitaux, coordonnée le 7 août 1987,
- l'arrêté royal du 3 mai 1999 déterminant les conditions générales auxquelles le dossier médical, visé à l'article 15 **(maintenant 20)** de la loi sur les hôpitaux, coordonnée le 7 août 1987, doit répondre,
- ainsi qu'à l'arrêté royal du 28 décembre 2006 déterminant les conditions générales minimales auxquelles le dossier infirmier, visé à l'article 17 quater **(maintenant 25)** de la loi relative aux hôpitaux, coordonnée le 7 août 1987, doit répondre (en vigueur le 1er août 2007).

Il doit aussi se référer aux différents dossiers décrits à l'annexe de l'arrêté royal du 23 octobre 1964 portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre.

Ensuite, les données à caractère personnel doivent être **exactes et, si nécessaire, mises à jour**. Il convient de se référer aux règles de l'art pour apprécier l'exactitude et la complétude des données faisant l'objet d'un traitement. La loi précise que toutes les mesures *raisonnables* doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées (art. 4, § 1er, 4°, de la loi du 8 décembre 1992). Au plus il est important d'avoir des données, au plus cette obligation sera lourde.

Enfin, la loi prévoit que les données ne peuvent être **conservées** sous une forme permettant l'identification des personnes concernées que pour une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement (art. 4, § 1er, 5°, de la loi du 8 décembre 1992). Le Roi a fixé les garanties permettant de conserver les données à caractère personnel au-delà de cette période, à des fins historiques, statistiques ou scientifiques (voyez le chapitre II de l'arrêté royal du 13 février 2001). Autrement dit, lorsque la finalité est réalisée, il n'y a plus de raison de conserver des données à caractère personnel et, par voie de conséquence, il n'est plus permis de les conserver sous une forme qui permette l'identification de la personne concernée.

La durée de conservation des données à caractère personnel s'apprécie dès lors au regard des finalités pour lesquelles elles ont été collectées et pour lesquelles elles seront traitées ultérieurement dans la mesure où ces finalités ultérieures sont compatibles, et des exigences légales ou réglementaires applicables. Ainsi, le délai de conservation minimal du dossier médical hospitalier est de trente ans tandis que le délai de conservation des données à caractère personnel en vue de défendre la responsabilité de l'hôpital sera déterminé en fonction de la prescription applicable. De même, le principe de qualité des données a pour conséquence que ces deux finalités n'imposeront pas nécessairement de conserver le même type d'information.

10.1.3.4. Droits de la personne concernée à l'égard du traitement de ses données à caractère personnel

La loi du 8 décembre 1992 reconnaît différents droits à la personne concernée à l'égard du traitement de ses données à caractère personnel :

1. Le droit de recevoir de l'information sur le traitement de ses données à caractère personnel ;
2. Un droit d'accès ;
3. Un droit de rectification à l'égard de toute donnée à caractère personnel inexacte qui la concerne ;
4. Un droit d'opposition au traitement de ses données à caractère personnel pour des raisons sérieuses et légitimes tenant à une situation particulière ;
5. Un droit d'opposition, gratuit et sans justification, au traitement de ses données à caractère personnel lorsque les données sont collectées à des fins de marketing direct ;
6. Le droit d'obtenir, sans frais, la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel la concernant qui, compte tenu du but (de la finalité) du traitement, est incomplète ou non pertinente ;
7. Le droit d'obtenir sans frais la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel la concernant dont l'enregistrement, la communication ou la conservation sont interdits ;
8. Le droit d'obtenir, sans frais, la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel la concernant qui a été conservée au-delà de la période autorisée ;
9. Le droit de ne pas être soumise à une décision produisant des effets juridiques à son encontre ou l'affectant de manière significative dans la mesure où cette décision aurait été prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, sauf exceptions ;
10. Le droit d'obtenir, à charge du responsable du traitement, la réparation du dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la loi, sauf à ce qu'il établisse que le fait générateur ne lui est pas imputable ;
11. Lorsque la légitimité du traitement de données à caractère personnel se fonde sur le consentement de la personne concernée, celle-ci a le droit de retirer son consentement à tout moment sans justification ni préavis.

Il faut déjà dire que le règlement relatif à la protection de la vie privée de l'hôpital doit indiquer la manière dont les patients peuvent exercer leurs droits visés dans la loi du 8 décembre 1992 relative à la protection de la vie privée a l'égard des traitements de données à caractère personnel (voyez sur ce point la disposition 9° quater de l'annexe à l'arrêté royal du 23 octobre 1964).

10.1.3.4.1. Le droit de recevoir de l'information sur le traitement des données à caractère personnel

Le droit de la personne à recevoir de l'information sur le traitement de données à caractère personnel qui la concerne ([50]) répond à une double exigence de transparence et de loyauté. Cette information participe à la « *volonté d'assurer à l'individu une transparence des circuits informationnels* (…) » ([51]). Elle représente aussi une facette de son droit à un traitement loyal de ses données ([52]). La personne concernée doit recevoir les éléments d'information nécessaires pour s'assurer du respect de la loi vie privée et de ses droits, et exercer les droits mis à sa disposition à cet effet. Ainsi, sans information adéquate, la personne concernée ne peut pas mettre en œuvre les droits qui lui sont reconnus tels que le droit d'accès, le droit de rectification ou le droit d'opposition.

Afin d'apprécier l'objet et la qualité de l'information, il convient de se référer au double objectif qui lui est ainsi assigné. A cet effet, l'information doit être *appropriée et adaptée aux circonstances* ([53]), ou, posé autrement, être *effective et complète* au regard des circonstances de la collecte des données auprès de la personne concernée ([54]), la première chose étant d'informer la personne concernée du l'existence du traitement de données à caractère personnel ([55]).

Pour être suffisante – et donc effective et concrète -, l'information du patient doit être spécifique à une situation déterminée et circonscrite tant dans son objet que dans ses effets. Ainsi, le responsable du traitement ne peut pas se contenter d'informer le patient que ses données pourraient faire l'objet d'un traitement à des fins scientifiques, statistiques ou historiques. Il doit au minimum préciser la nature du projet, les objectifs de celui-ci, ainsi que le nom de la personne ou de l'organisme pour le compte duquel est effectuée la recherche ([56]).

Le non-respect de l'obligation d'informer la personne concernée est passible d'une amende de 100 à 100.000 EUR (+ application des décimes additionnels).

---

[50] Art. 9 de la loi du 8 décembre 1992. Sur le droit d'information, voyez not. : D. DE BOT, *Verwerking van persoonsgegevens*, Antwerpen, Kluwer, 2001, pp. 188-211, n° 255-280.

[51] M.-H. BOULANGER, C. DE TERWANGNE et Th. LEONARD, « La protection de la vie privée à l'égard des traitements de données à caractère personnel », *J.T.*, 1993, p. 382, n° 65.

[52] Sur l'exigence de loyauté, voyez not. : Th. LEONARD et Y. POULLET, *o.c.*, p. 385, n° 28 ; *Manuel de la vie privée*, Bruxelles, Ed. Politieia, p. 64.

[53] Rec. n° R (97) 5, *o.c.*, art. 5.3.

[54] Considérant 38 de la directive 95/46/CE.

[55] Considérant 38 de la directive 95/46/CE ; Rec. n° R (97) 5, *o.c.*, art. 5.1.a. De manière analogue : Exp. motifs précédant le projet ayant donné lieu à la loi du 8 décembre 1992, Doc. Parl., Ch., *s.o.*, 1990-1991, n° 1601-1, p. 15. Voir aussi : Comm. Pr. Vie privée, avis du 6 août 1993, n° 09/93 : « *Le législateur a inséré l'obligation d'informer l'intéressé de son premier enregistrement dans un traitement, pour qu'il soit au courant de l'existence d'un traitement comprenant des données le concernant*. »

[56] Rec. n° R (83)10, *o.c.*, art. 3.1.

Dans certains cas, le patient a le droit d'obtenir une information spécifique à raison d'une règle juridique particulière. Ainsi, conformément à la théorie du secret partagé, le patient doit pouvoir *s'opposer à tout moment à la communication* de ses données d'un praticien à l'autre. Cela implique que le patient doit être *préalablement informé* de toute communication effective entre professionnels, ou à tout le moins des modalités de fonctionnement des réseaux impliquant des transferts « potentiels » de données entre professionnels ([57]).

La loi du 8 décembre 1992 distingue selon que les données à caractère personnel sont ou non obtenues auprès de la personne concernée.

10.1.3.4.1.1. Les données à caractère personnel sont obtenues auprès de la personne concernée

10.1.3.4.1.1.1. Le moment de l'information

Lorsque les données sont obtenues auprès de la personne concernée, le responsable du traitement (ou son représentant) doit lui fournir l'information requise au plus tard au moment où il les obtient (art. 9, § 1er, de la loi du 8 décembre 1992).

10.1.3.4.1.1.2. Le contenu de l'information

L'information doit porter au moins sur les informations suivantes (art. 9, § 1er, de la loi du 8 décembre 1992) :

a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant ;
b) les finalités du traitement ;
c) l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de direct marketing ;
d) d'autres informations supplémentaires, notamment:
   - les destinataires ou les catégories de destinataires des données,
   - le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse,
   - l'existence d'un droit d'accès et de rectification des données la concernant; sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont obtenues, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

---

57 J. HERVEG, M.-N. VERHAEGEN et Y. POULLET, o.c., n° 19.

En application de l'article 25, 4°, de l'arrêté royal du 13 février 2001, en présence de données médicales, le responsable du traitement doit en outre mentionner la base légale ou réglementaire qui autorise leur traitement.

L'article 26 de ce même arrêté impose que, lorsque le traitement de données médicales est exclusivement autorisé par le consentement écrit de la personne concernée, le responsable du traitement doit, en outre et préalablement au traitement :

- communiquer à la personne concernée les motifs pour lesquels ces données sont traitées,
- ainsi que la liste des catégories de personnes ayant accès à ces données.

10.1.3.4.1.1.3. L'exception à l'obligation d'information

Le responsable est délivré de l'obligation d'informer la personne concernée lorsque celle-ci est déjà informée de ces éléments (art. 9, § 1er, de la loi du 8 décembre 1992).

10.1.3.4.1.2. Les données à caractère personnel ne sont pas obtenues auprès de la personne concernée

10.1.3.4.1.2.1. Le moment de l'information

Lorsque les données n'ont pas été obtenues auprès de la personne concernée, l'information doit être fournie à la personne concernée soit (art. 9, § 2, de la loi du 8 décembre 1992) :

- dès l'enregistrement des données ;
- ou, si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données.

10.1.3.4.1.2.2. Le contenu de l'information

L'information doit porter au moins sur les informations suivantes (art. 9, § 2, al. 1, de la loi du 8 décembre 1992) :

a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant ;
b) les finalités du traitement ;
c) l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de direct marketing; dans ce cas, la personne concernée doit être informée avant que des données à caractère personnel ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de direct marketing ;
d) d'autres informations supplémentaires, notamment :

- les catégories de données concernées ;
- les destinataires ou les catégories de destinataires ;
- l'existence d'un droit d'accès et de rectification des données la concernant; sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont traitées, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données ;

En application de l'article 25, 4°, de l'arrêté royal du 13 février 2001, en présence de données médicales, le responsable du traitement doit en outre mentionner la base légale ou réglementaire qui autorise leur traitement.

L'article 26 de ce même arrêté impose que, lorsque le traitement de données médicales est exclusivement autorisé par le consentement écrit de la personne concernée, le responsable du traitement doit, en outre et préalablement au traitement :

- communiquer à la personne concernée les motifs pour lesquels ces données sont traitées,
- ainsi que la liste des catégories de personnes ayant accès à ces données.

10.1.3.4.1.2.3. Les exceptions à l'obligation d'information

10.1.3.4.1.2.3.1. Le responsable est délivré de l'obligation d'informer la personne concernée lorsque celle-ci est déjà informée de ces éléments (art. 9, § 2, al. 1, de la loi du 8 décembre 1992).

10.1.3.4.1.2.3.2. Le responsable du traitement est dispensé de fournir les informations visées à l'article 9, § 2, de la loi du 8 décembre 1992 (art. 9, § 2, al. 2, de la loi du 8 décembre 1992) :

a) Lorsque, en particulier pour un traitement aux fins de statistiques ou de recherche historique ou scientifique ou pour le dépistage motivé par la protection et la promotion de la santé publique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés.

   Quand le responsable du traitement entend se prévaloir de cette exemption, il doit justifier cette impossibilité dans la déclaration du traitement à notifier à la Commission de la protection de la vie privée en application de l'article 17 de la loi du 8 décembre 1992 (art. 31, al. 1, de l'arrêté royal du 13 février 2001). La Commission publie la liste des responsables de traitement qui bénéfice de cette dispense. Cette liste est reprise dans le registre public tenu par la Commission en application de l'article 18 de la loi du 8 décembre 1992 (art. 31, al. 2, de l'arrêté royal du 13 février 2001).

Si le responsable du traitement entre en contact avec la personne concernée, il doit alors lui fournir ces informations. En effet, dans cette hypothèse, l'impossibilité d'informer ne se justifie plus (art. 28 de l'arrêté royal du 13 février 2001).

De même, si le tiers auquel le responsable du traitement a communiqué les données à caractère personnel entre en contact avec la personne concernée, ce tiers doit lui fournir ces informations puisque, de nouveau, l'impossibilité d'informer ne se justifie plus (art. 28 de l'arrêté royal du 13 février 2001).

b) Lorsque l'enregistrement ou la communication des données à caractère personnel est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

10.1.3.4.1.2.3.3. Le responsable du traitement ultérieur à des fins historiques, statistiques ou scientifiques qui traite exclusivement des données codées est exempté de l'obligation d'information instituée à l'article 9, § 2, de la loi du 8 décembre 1992, à condition de respecter les dispositions relatives au traitement de données à caractère personnel codées fixées aux articles 7 à 17 de l'arrêté royal du 13 février 2001 (art. 28 de l'arrêté royal du 13 février 2001).

10.1.3.4.1.2.3.4. Cet arrêté prévoit aussi que lorsqu'une autorité administrative est chargée explicitement par ou en vertu de la loi de rassembler et de coder les données à caractère personnel et est soumise à cet égard à des mesures spécifiques visant à protéger la vie privée instituées par ou en vertu de la loi, elle est exemptée de l'obligation d'information instituée par l'article 9 § 2 de la loi lorsqu'elle agit en tant qu'organisation intermédiaire (art. 29 de l'arrêté royal du 13 février 2001).

10.1.3.4.1.3. La forme de cette information dans un hôpital : le règlement relatif à la protection de la vie privée ?

L'hôpital doit communiquer aux patients les dispositions du règlement relatif à la protection de la vie privée qu'il doit tenir en application de l'arrêté royal du 23 octobre 1964 portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre, modifié sur ce point après l'adoption de la loi du 8 décembre 1992. Il faut rappeler que ces dispositions n'ont pas été modifiées suite à la transposition de la directive 95/46/CE et qu'elles se réfèrent toujours à la version initiale de la loi du 8 décembre 1992. Ni la loi ni l'arrêté royal ne précisent si ce règlement s'ajoute à ou remplace l'information due en application de l'article 9 de la loi du 8 décembre 1992. D'un côté, il pourrait être soutenu que la loi postérieure déroge à la loi antérieure, ce qui pourrait induire la disparition des obligations relatives à ce règlement. D'un autre côté, il pourrait être soutenu que la loi spéciale déroge à la loi générale.

En tout cas, le règlement relatif à la protection de la vie privée doit comporter au moins les indications suivantes, fournissant de la sorte une plus large information que celle visée à l'article 9 de la loi du 8 décembre 1992 :

- les finalités du traitement ;
- le cas échéant, la loi, le décret, l'ordonnance ou l'acte réglementaire décidant la création du traitement automatisé ;
- l'identité et l'adresse du « maître du fichier » et de la personne qui peut agir en son nom ;
- le nom du médecin qui exerce la responsabilité et la surveillance visées à l'article 7, alinéa 1er, de la version initiale de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ;
- le nom du conseiller en sécurité chargé de la sécurité de l'information ;
- l'identité et l'adresse du (des) « gestionnaire(s) » de traitements ;
- les droits et obligations du (des) « gestionnaire(s) » de traitements ;
- les catégories de personnes ayant accès ou étant autorisées à obtenir les données médicales à caractère personnel du traitement ;
- les catégories de personnes dont les données font l'objet d'un traitement ;
- la nature des données traitées et la manière dont elles sont obtenues ;
- l'organisation du circuit des données médicales à traiter ;
- la procédure suivant laquelle, si nécessaire, les données sont rendues anonymes ;
- les procédures de sauvegarde afin d'empêcher la destruction accidentelle ou illicite de données, la perte accidentelle de données ou l'accès illicite à celles-ci, leur modification ou diffusion illicite ;
- le délai au-delà duquel les données ne peuvent plus, le cas échéant, être gardées, utilisées ou diffusées ;
- les rapprochements, interconnexions ou tout autre forme de mise en relation de données l'objet du traitement ;
- les interconnexions et les consultations ;
- les cas où des données sont effacées ;
- la manière dont les patients peuvent exercer leurs droits visés dans la loi du 8 décembre 1992 relative à la protection de la vie privée a l'égard des traitements de données à caractère personnel.

Ce règlement doit aussi mentionner le numéro d'identification du traitement auquel il se rapporte, tel qu'il est attribué par la Commission de la protection de la vie privée.

En outre, ce règlement doit être transmis à la Commission pour la supervision et l'évaluation des données statistiques qui concernent les activités médicales dans les hôpitaux. Toutes les modifications apportées au règlement précité doivent être transmises, dans les trente jours de leur ratification par les instances compétences du pouvoir organisateur, à la Commission pour la supervision et l'évaluation des données statistiques qui concernent les activités médicales dans les hôpitaux. La Commission pour la supervision et l'évaluation des données statistiques

qui concernent les activités médicales dans les hôpitaux, tient ces règlements à la disposition de la Commission de la protection de la vie privée et lui communique tous les six mois la liste actualisée des règlements reçus et des modifications de règlements qu'il a reçus.

10.1.3.4.2. Le droit d'accès

10.1.3.4.2.1. L'objet du droit d'accès

Le droit d'accès de la personne concernée ([58]) porte sur les éléments suivants ([59]) :

1. La confirmation que des données la concernant sont ou ne sont pas traitées.
2. Des informations portant au moins sur :
   - les finalités du traitement,
   - les catégories de données sur lesquelles le traitement porte,
   - et les catégories de destinataires auxquels les données sont communiquées.
3. La communication, sous une forme intelligible, des données faisant l'objet des traitements.
4. La communication de toute information disponible sur l'origine des données faisant l'objet des traitements.
5. La connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, dans le cas des décisions automatisées visées à l'article 12 bis de la loi du 8 décembre 1992.
6. Un avertissement de la faculté d'exercer les recours prévus aux articles 12 ([60]) et 14 ([61]) et, éventuellement, de consulter le registre public prévu à l'article 18 de la loi du 8 décembre 1992.
7. La prise de connaissance des données à caractère personnel traitées en ce qui concerne sa santé, soit directement, soit avec l'aide d'un praticien professionnel en soins de santé, et ce, sans préjudice de l'article 9, § 2, de la loi du 22 août 2002 relative aux droits du patient. Le responsable du traitement ne peut pas imposer à la personne concernée de prendre connaissance de ces données par l'intermédiaire d'un professionnel des soins de santé ([62]).
8. La communication des données à caractère personnel traitées en ce qui concerne sa santé, par l'intermédiaire d'un professionnel des soins de santé choisi par la personne concernée, à la demande du responsable du traitement ou de la personne concernée,

---

[58] Art. 10 de la loi du 8 décembre 1992. A propos de ce droit, voyez not., **pour l'art. 10, § 1, de la loi :** D. DE BOT, o.c., pp. 222-236, n° 298-317 ; Th. LEONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution, La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, p. 389, n° 47, **et, pour l'article 10, § 2, de la loi** : J. HERVEG, M.-N. VERHAEGEN et Y. POULLET, « Les droits du patient face au traitement informatisé de ses données dans une finalité thérapeutique : les conditions d'une alliance entre informatique, vie privée et santé », *Rev. dr. Santé*, 2002-2003/2, n° 50.

[59] Sur l'accès au dossier médical, voyez l'article 9, § 2, de la loi du 22 août 2002 relative aux droits du patient et not. : S. CALLENS et S. DE WILDE, « L'accès au dossier médical : un nouveau droit », in G. SCHAMPS (dir.), *Evolution des droits du patient, indemnisation sans faute des dommages liés aux soins de santé : le droit médical en mouvement*, Bruxelles, Bruylant, Paris, L.G.D.J., 2008, p. 159.

[60] Droit de rectification, droit d'opposition et droit d'obtenir la suppression ou l'interdiction d'utilisation de certaines données.

[61] Recours comme en référé devant le Président du tribunal de première instance.

[62] J. HERVEG, M.-N. VERHAEGEN et Y. POULLET, o.c., n° 52.

toujours sans préjudice de l'article 9, § 2, de la loi du 22 août 2002 relative aux droits du patient.

Il faut rappeler que l'arrêté royal du 3 mai 1999 déterminant les conditions générales minimales auxquelles le dossier médical, visé à l'article 15 **(maintenant 20)** de la loi relative aux hôpitaux, coordonnée le 7 août 1987, doit répondre, prévoit toujours que « *Le patient ou son représentant légal a le droit de prendre connaissance, par l'intermédiaire d'un médecin choisi par lui, des données du dossier médical qui le concernent* » ([63]).

Le non-respect du droit d'accès visé à l'article 10, § 1er, de la loi du 8 décembre 1992 est passible d'une amende de 100 à 100.000 EUR (+ application des décimes additionnels).

10.1.3.4.2.2. L'exercice du droit d'accès

Pour obtenir la communication de l'information visée à l'article 10 de la loi du 8 décembre 1992 ([64]), la personne concernée doit justifier son identité ([65]) et adresser une demande datée et signée qu'elle remet sur place ou qu'elle envoie par la poste ou par tout moyen de télécommunication, soit au responsable du traitement ou à son représentant en Belgique ou à l'un de ses mandataires ou préposés, soit au sous-traitant du traitement des données à caractère personnel qui la communique, le cas échéant, à une des personnes mentionnées ci-dessus ([66]).

En cas de remise de la demande sur place, la personne qui la reçoit délivre immédiatement un accusé de réception daté et signé à l'auteur de la demande ([67]).

Les renseignements doivent être communiqués sans délai et au plus tard *dans les quarante-cinq jours* de la réception de la demande ([68]). Cependant, formellement, cette dernière exigence et le délai maximal de quarante-cinq jours n'existent pas pour le droit de prendre connaissance et le droit d'obtenir communication des données médicales ([69]). Il devrait par conséquent y être fait droit immédiatement.

---

63 Sur ce problème, voyez : J. HERVEG, M.-N. VERHAEGEN et Y. POULLET, o.c., n° 56.

64 La procédure est fixée par l'art. 10, § 1, al. 2 à 4, de la loi du 8 décembre 1992, précisée par l'art. 32 de l'arrêté royal du 13 février 2001. Voyez à ce sujet : C. de TERWANGNE et S. LOUVEAUX, « Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal », *J.T.*, 2001, p. 461 et s.

65 La personne concernée doit apporter la preuve de son identité (Loi du 8 déc. 1992, art. 10, § 1, al. 1).

66 Art. 32, al. 1, de l'arrêté royal du 13 février 2001.

67 Art. 32, al. 2, de l'arrêté royal du 13 février 2001.

68 Art. 10, § 1, al. 3, de l'arrêté royal du 13 février 2001.

69 En effet, si les autres conditions sont reprises pour les données médicales à l'article 32 de l'arrêté royal, par contre, l'exigence d'une communication sans délai des renseignements et au plus tard dans les 45 jours de la demande n'est reprise que pour l'exercice du droit visé à l'article 10, § 1, de la loi du 8 décembre 1992.

Lorsque les données relatives à la santé de la personne concernée sont traitées aux fins de recherches médico-scientifiques, qu'il est manifeste qu'il n'existe aucun risque qu'il soit porté atteinte à la vie privée de cette personne et que les données ne sont pas utilisées pour prendre des mesures à l'égard d'une personne concernée individuelle, la communication peut, pour autant qu'elle soit susceptible de nuire gravement auxdites recherches, être différé au plus tard jusqu'à l'achèvement des recherches. Dans ce cas, la personne concernée doit avoir préalablement donné son autorisation écrite au responsable du traitement que les données à caractère personnel la concernant peuvent être traitées à des fins médico-scientifiques et que la communication de ces données peut dès lors être différée. (art. 10, § 2, al. 3, de la loi du 8 décembre 1992).

La loi précise qu'il ne doit être donné suite à une demande d'accès à ses données à caractère personnel qu'à l'expiration d'un délai raisonnable, à compter de la date d'une demande antérieure d'une même personne à laquelle il a été répondu ou de la date à laquelle les données lui ont été communiquées d'office ([70]). Le but est d'éviter que le responsable du traitement ne doive faire face à des demandes d'accès répétées et abusives.

10.1.3.4.3. Le droit de rectification

Toute personne a le droit d'obtenir sans frais la rectification de toute donnée à caractère personnel *inexacte* qui la concerne (art. 12, § 1er, al. 1, de la loi du 8 décembre 1992).

Ainsi que l'explique Thierry LEONARD ([71]), l'inexactitude d'une information se décline de trois façons :

- soit l'information n'est pas exacte objectivement ; elle n'est pas conforme à la réalité ;
- soit l'information n'est pas à jour, actuelle ;
- soit l'information n'est pas complète.

Pour obtenir la rectification, la suppression ou l'interdiction d'utilisation de la donnée à caractère personnel inexacte qui la concerne ([72]), sans frais à sa charge ([73]), la personne concernée doit justifier son identité et adresser une demande datée et signée qu'elle remet sur place ou qu'elle envoie par la poste ou par tout moyen de télécommunication, soit au responsable du traitement ou à son représentant en Belgique ou à l'un de ses mandataires ou préposés, soit au sous-traitant du traitement des données à caractère personnel qui la communique, le cas échéant, à une des personnes mentionnées ci-dessus ([74]).

---

70 Art. 10, § 3, de la loi du 8 décembre 1992.

71 Th. LEONARD, obs. sous Civ. Bruxelles (Prés.), 22 mars 1994, *J.T.*, 1994, p. 845, n° 11.

72 La procédure est fixée par l'art. 12, §§ 2 et 3, de la loi du 8 décembre 1992, précisée par l'art. 33 de l'arrêté royal du 13 février 2001 (qui renvoie à la procédure déterminée à l'art. 32). Voyez aussi à ce sujet : C. de TERWANGNE et S. LOUVEAUX, o.c., *J.T.*, 2001, p. 461 et s.

73 Art. 12, § 1, al. 1, de la loi du 8 décembre 1992.

74 Art. 32, al. 1, de l'arrêté royal du 13 février 2001.

En cas de remise de la demande sur place, la personne qui la reçoit délivre immédiatement un accusé de réception daté et signé à l'auteur de la demande ([75]).

Dans le mois qui suit l'introduction de la requête, le responsable du traitement communique les rectifications ou effacements des données, effectués sur base de l'article 12, § 1, de la loi du 8 décembre 1992. Cette communication doit être adressée à la personne concernée ainsi qu'aux personnes à qui les données inexactes ont été communiquées, pour autant qu'il ait encore connaissance des destinataires de la communication et que la notification à ces destinataires ne paraisse pas impossible ou n'implique pas des efforts disproportionnés ([76]).

Dès la réception de la demande de rectification, le responsable du traitement doit indiquer clairement, lors de toute communication, que la donnée est contestée (art. 15 de la loi du 8 décembre 1992). Le non-respect de cette obligation est passible d'une amende de 100 à 20.000 EUR (+ application des décimes additionnels).

10.1.3.4.4. Le droit d'opposition au traitement de ses données à caractère personnel pour des raisons sérieuses et légitimes tenant à une situation particulière

Toute personne a le droit de s'opposer, pour des raisons sérieuses et légitimes tenant à une situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, (art. 12, § 1er, al. 2, de la loi du 8 décembre 1992).

La personne concernée ne peut pas s'opposer au traitement (art. 12, § 1er, al. 2, de la loi du 8 décembre 1992) :

- lorsqu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- lorsqu'il est nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

La mise en œuvre de ce droit est délicate notamment lorsque le patient s'oppose à l'insertion de données le concernant dans le dossier médical ou infirmier hospitalier qui constitue de l'autre côté une obligation dans le chef de l'hôpital et des praticiens des soins de santé.

Pour obtenir la rectification, la suppression ou l'interdiction d'utilisation de la donnée à caractère personnel toute donnée à caractère personnel au traitement de laquelle elle s'est opposée ([77]), la personne concernée doit justifier son identité et adresser une demande datée et

---

75 Art. 32, al. 2, de l'arrêté royal du 13 février 2001.

76 Art. 12, § 3, al. 1, de la loi du 8 décembre 1992.

77 La procédure est fixée par l'art. 12, §§ 2 et 3, de la loi du 8 décembre 1992, précisée par l'art. 33 de l'arrêté royal du 13 février 2001 (qui renvoie à la procédure déterminée à l'art. 32). Voyez aussi à ce sujet : C. de TERWANGNE et S. LOUVEAUX, o.c., *J.T.*, 2001, p. 461 et s.

signée qu'elle remet sur place ou qu'elle envoie par la poste ou par tout moyen de télécommunication, soit au responsable du traitement ou à son représentant en Belgique ou à l'un de ses mandataires ou préposés, soit au sous-traitant du traitement des données à caractère personnel qui la communique, le cas échéant, à une des personnes mentionnées ci-dessus ([78]).

En cas de remise de la demande sur place, la personne qui la reçoit délivre immédiatement un accusé de réception daté et signé à l'auteur de la demande ([79]).

Dans le mois qui suit l'introduction de la requête, le responsable du traitement communique à la personne concernée la suite réservée à sa demande ([80]).

Lorsque l'opposition au traitement des données est justifiée, le traitement mis en œuvre par le responsable du traitement ne peut plus porter sur ces données (art. 12, § 1, al. 4, de la loi du 8 déc. 1992).

10.1.3.4.5. Le droit d'opposition, gratuit et sans justification, au traitement de ses données à caractère personnel lorsque les données sont collectées à des fins de marketing direct

Lorsque les données à caractère personnel sont collectées à des fins de direct marketing, toute personne peut s'opposer, gratuitement et sans aucune justification, au traitement projeté de données à caractère personnel la concernant (art. 12, § 1er, al. 3, de la loi du 8 décembre 1992).

Pour obtenir la rectification, la suppression ou l'interdiction d'utilisation de la donnée à caractère personnel toute donnée à caractère personnel au traitement de laquelle elle s'est opposée ([81]), sans frais à sa charge ([82]), la personne concernée doit justifier son identité et adresser une demande datée et signée qu'elle remet sur place ou qu'elle envoie par la poste ou par tout moyen de télécommunication, soit au responsable du traitement ou à son représentant en Belgique ou à l'un de ses mandataires ou préposés, soit au sous-traitant du traitement des données à caractère personnel qui la communique, le cas échéant, à une des personnes mentionnées ci-dessus ([83]).

---

78 Art. 32, al. 1, de l'arrêté royal du 13 février 2001.

79 Art. 32, al. 2, de l'arrêté royal du 13 février 2001.

80 Art. 12, § 3, al. 2, de la loi du 8 décembre 1992.

81 La procédure est fixée par l'art. 12, §§ 2 et 3, de la loi du 8 décembre 1992, précisée par l'art. 33 de l'arrêté royal du 13 février 2001 (qui renvoie à la procédure déterminée à l'art. 32). Voyez aussi à ce sujet : C. de TERWANGNE et S. LOUVEAUX, o.c., *J.T.*, 2001, p. 461 et s.

82 Art. 12, § 1, al. 3, de la loi du 8 décembre 1992.

83 Art. 32, al. 1, de l'arrêté royal du 13 février 2001.

En cas de remise de la demande sur place, la personne qui la reçoit délivre immédiatement un accusé de réception daté et signé à l'auteur de la demande ([84]).

Dans le mois qui suit l'introduction de la requête, le responsable du traitement communique à la personne concernée la suite réservée à sa demande ([85]).

Lorsque l'opposition au traitement des données est justifiée, le traitement mis en œuvre par le responsable du traitement ne peut plus porter sur ces données (art. 12, § 1, al. 4, de la loi du 8 déc. 1992).

10.1.3.4.6. Le droit d'obtenir, sans frais, la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel la concernant qui, compte tenu du but (de la finalité) du traitement, est incomplète ou non pertinente

Toute personne a le droit d'obtenir sans frais la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel la concernant qui, compte tenu du but du traitement, est incomplète ou non pertinente (art. 12, § 1er, al. 5, de la loi du 8 décembre 1992).

Afin d'apprécier le caractère incomplet ou non pertinent des données à caractère personnel, compte tenu du but de leur traitement, il faut recourir au principe de proportionnalité et, à cet effet, pondérer les intérêts, droits ou libertés en présence ([86]).

En tout cas, les données à caractère personnel sont incomplètes lorsqu'elles ne donnent pas une image suffisante de la personne concernée au regard de la finalité poursuivie par leur traitement ([87]).

De même, les données à caractère personnel ne sont pas pertinentes lorsqu'elles ne présentent pas un caractère de nécessité pour la réalisation de la finalité du traitement de données ([88]).

En d'autres mots, les données doivent être adéquates, pertinentes et non excessives par rapport à la finalité poursuivie, ce qui renvoie au principe de qualité des données traitées.

---

84 Art. 32, al. 2, de l'arrêté royal du 13 février 2001.

85 Art. 12, § 3, al. 2, de la loi du 8 décembre 1992.

86 Th. LEONARD, o.c., *J.T.*, 1994, p. 845, n° 11.

87 Th. LEONARD, o.c. ; D. DE BOT, o.c., p. 354, n° 498. Thierry LEONARD donne pour exemple le cas d'une mutuelle d'informations où les informations ne sont pas suffisantes pour éviter un problème d'homonymie dont les conséquences, eu égard à la finalité poursuivie, seraient « catastrophiques » pour la personne concernée (note infra-paginale n° 28). Dirk DE BOT ajoute un exemple dans le secteur du crédit à la consommation où la personne concernée peut exiger que les raisons des non-paiements soient prises en compte dans le cadre d'un traitement de données relatives à des retards de paiement.

88 D. DE BOT, o.c., p. 355, n° 498 : ainsi, par exemple, il n'est pas pertinent de traiter les revenus professionnels des parents d'une personne majeure sollicitant un prêt lors de l'évaluation de sa capacité de remboursement.

Pour obtenir la rectification, la suppression ou l'interdiction d'utilisation de la donnée à caractère personnel incomplète ou non pertinente, compte tenu du but du traitement ([89]), sans frais à sa charge ([90]), la personne concernée doit justifier son identité et adresser une demande datée et signée qu'elle remet sur place ou qu'elle envoie par la poste ou par tout moyen de télécommunication, soit au responsable du traitement ou à son représentant en Belgique ou à l'un de ses mandataires ou préposés, soit au sous-traitant du traitement des données à caractère personnel qui la communique, le cas échéant, à une des personnes mentionnées ci-dessus ([91]).

En cas de remise de la demande sur place, la personne qui la reçoit délivre immédiatement un accusé de réception daté et signé à l'auteur de la demande ([92]).

Dans le mois qui suit l'introduction de la requête, le responsable du traitement communique les rectifications ou effacements des données, effectués sur base de l'article 12, § 1, de la loi du 8 décembre 1992. Cette communication doit être adressée à la personne concernée ainsi qu'aux personnes à qui les données incomplètes ou non pertinentes ont été communiquées, pour autant qu'il ait encore connaissance des destinataires de la communication et que la notification à ces destinataires ne paraisse pas impossible ou n'implique pas des efforts disproportionnés ([93]).

Dès la réception de la demande de suppression ou d'interdiction d'utilisation, le responsable du traitement doit indiquer clairement, lors de toute communication, que la donnée est contestée (art. 15 de la loi du 8 décembre 1992). Le non-respect de cette obligation est passible d'une amende de 100 à 20.000 EUR (+ application des décimes additionnels).

10.1.3.4.7. Le droit d'obtenir sans frais la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel la concernant dont l'enregistrement, la communication ou la conservation sont interdits

Toute personne a le droit d'obtenir sans frais la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel la concernant dont l'enregistrement, la communication ou la conservation sont interdits (art. 12, § 1er, al. 5, de la loi du 8 décembre 1992).

Tout manquement à toute disposition prise par ou en vertu de la loi implique-t-il l'interdiction du traitement ? Ou le manquement ne peut-il être que relatif aux conditions générales de licéité ? Le défaut de déclaration du traitement à la Commission de protection de la vie privée entraîne-t-il l'interdiction du traitement ?

---

89 La procédure est fixée par l'art. 12, §§ 2 et 3, de la loi du 8 décembre 1992, précisée par l'art. 33 de l'arrêté royal du 13 février 2001 (qui renvoie à la procédure déterminée à l'art. 32). Voyez aussi à ce sujet : C. de TERWANGNE et S. LOUVEAUX, o.c., *J.T.*, 2001, p. 461 et s.

90 Art. 12, § 1, al. 5, de la loi du 8 décembre 1992.

91 Art. 32, al. 1, de l'arrêté royal du 13 février 2001.

92 Art. 32, al. 2, de l'arrêté royal du 13 février 2001.

93 Art. 12, § 3, al. 1, de la loi du 8 décembre 1992.

En réalité, il faut pouvoir se prévaloir, d'une manière ou d'une autre, d'une prohibition expresse dans la loi du 8 décembre 1992 ou un de ses arrêtés d'exécution ou en vertu des principes qui y sont énoncés.

Un *premier exemple* est le traitement ultérieur de données à caractère personnel à des fins incompatibles avec les finalités déterminées, explicites et légitimes pour lesquelles elles avaient été collectées initialement, donc, par exemple, en méconnaissance des règles fixées par l'arrêté royal du 13 février 2001 pour les traitements ultérieurs de données à des fins historiques, statistiques ou scientifiques.

Un *second exemple* est le traitement de données en dehors des hypothèses de légitimation des traitements de données telles que décrites aux articles 5 à 8 de la loi du 8 décembre 1992 ([94]).

Un *troisième exemple* est le traitement de données effectué en violation des règles propres aux données traitées ([95]).

Un *quatrième exemple* est le non-respect de l'interdiction de prendre une décision produisant des effets juridiques produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative sur le seul fondement de données destiné à évaluer certains aspects de sa personnalité ([96]).

D'autres interdictions peuvent encore être trouvées notamment en matière de transfert de données à caractère personnel vers des pays non-membres de la Communauté européenne ([97]).

Par contre, le traitement n'est pas interdit au motif qu'il n'a pas été déclaré auprès de la Commission de protection de la vie privée, pas plus qu'en cas de manquement à l'obligation d'informer la personne concernée ([98]) ou aux obligations à prendre pour assurer la sécurité et la confidentialité du traitement de données à caractère personnel.

---

94 Ce qui ne semble pas viser la méconnaissance des articles 25 à 27 de l'arrêté royal du 13 février 2001.

95 Ce qui renvoie au principe de licéité du traitement de données. Ainsi, par exemple, le médecin généraliste gestionnaire d'un dossier médical général / global ne peut pas transmettre les données relatives à son patient aux collègues qui traitent également le patient, sans le consentement du patient (art. 4, § 1, de l'arrêté royal du 3 mai 1999 relative au dossier médical général). S'il le fait quand même, c'est une communication de donnée illicite et, par conséquent, interdite par la loi du 8 décembre 1992. Le même raisonnement peut être suivi en cas de violation des règles relatives au secret professionnel.

96 L'article 12 bis, alinéa 2, de la loi du 8 déc. 1992, précise que « *L'interdiction prévue à l'alinéa 1er ne s'applique pas lorsque la décision est prise dans le cadre d'un contrat ou est fondée sur une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance. Ce contrat ou cette disposition doivent contenir des mesures appropriées, garantissant la sauvegarde des intérêts légitimes de l'intéressé. Il devra au moins être permis à celui-ci de faire valoir utilement son point de vue.* ». Il s'agit donc d'une interdiction expresse. Contra : D. DE BOT, o.c., p. 356, n° 501.

97 Voyez l'article 22, § 2, de la loi du 8 déc. 1992.

98 Th. LEONARD, o.c., *J.T.*, 1994, p. 846, n° 11.

Mais le traitement de données à caractère personnel qui présente des risques particuliers pour les droits et libertés ([99]) et qui n'a pas fait l'objet d'un examen préalable, constitue-t-il un traitement interdit ? La directive 95/46/CE impose aux Etats membres de préciser les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et de veiller à ce qu'ils soient examinés avant leur mise en œuvre ([100]). Il ne faut pas s'y méprendre ; la directive impose bien l'obligation aux Etats membres d'identifier ces traitements et de veiller à leur examen préalable ([101]). Les risques particuliers sont ceux qui résultent de la nature même du traitement poursuivi, de sa portée ou de ses finalités ([102]). La directive donne pour exemple des finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat. Ces risques particuliers peuvent aussi résulter de l'usage particulier d'une technologie nouvelle ([103]). La directive insiste sur le fait que, au regard de tous les traitements mis en œuvre dans la société, le nombre de ceux présentant de tels risques devrait être très restreint ([104]). En droit belge, le Roi a reçu la mission de déterminer les catégories de traitements qui présentent de tels risques et de fixer les conditions particulières pour garantir les droits et libertés des personnes concernées, après avis de la Commission de protection de la vie privée ([105]). Mais pour établir le caractère interdit de ce traitement, la personne concernée doit pouvoir établir la violation d'une prohibition expresse contenue soit dans la loi du 8 décembre 1992 soit dans un de ses arrêtés d'exécution ou fondée sur des principes qui y sont énoncés. Pour rappel, la Commission de protection de la vie privée n'a pas le pouvoir d'autoriser ou d'interdire un traitement de données. Dans les faits, c'est d'abord les caractères de légitimité et de licéité du traitement de données qui seront au cœur des débats.

Pour obtenir la suppression ou l'interdiction d'utilisation de la donnée à caractère personnel dont l'enregistrement, la communication ou la conservation sont interdits ([106]), sans frais à sa charge ([107]), la personne concernée doit justifier son identité et adresser une demande datée et signée qu'elle remet sur place ou qu'elle envoie par la poste ou par tout moyen de télécommunication, soit au responsable du traitement ou à son représentant en Belgique ou à

---

99 Comme la constitution de listes noires en matière d'assurances ou de location immobilière.

100 Art. 20 de la directive 95/46/CE. Voyez cependant la formulation des considérants 53 et 54. Pourrait-on reconnaître un effet direct à cette disposition ? La réponse est incertaine. Cependant, la Cour de Justice de Luxembourg a déjà reconnu un effet direct aux articles 6, § 1, c, et 7, c et e (C.J.C.E., arrêt du 20 mai 2003, affaires jointes C-465/00, C-138/01 et C-139/01, *Recueil*, 2003, p. I-04989, §§ 98 à 101).

101 En ce sens : M.-H. BOULANGER, C. de TERWANGNE, Th. LEONARD, S. LOUVEAUX, D. MOREAU et Y. POULLET, « La protection des données à caractère personnel en droit européen », *J.T.D.E.,* 1997, p. 152, n° 62.

102 Considérant 53 de la directive 95/46/CE.

103 Idem.

104 Considérant 54 de la directive 95/46/CE. Cette affirmation peut-elle être toujours maintenue ?

105 Art. 17 bis, al. 1, de la loi du 8 décembre 1992.

106 La procédure est fixée par l'art. 12, §§ 2 et 3, de la loi du 8 décembre 1992, précisée par l'art. 33 de l'arrêté royal du 13 février 2001 (qui renvoie à la procédure déterminée à l'art. 32). Voyez aussi à ce sujet : C. de TERWANGNE et S. LOUVEAUX, o.c., *J.T.*, 2001, p. 461 et s.

107 Art. 12, § 1, al. 5, de la loi du 8 décembre 1992.

l'un de ses mandataires ou préposés, soit au sous-traitant du traitement des données à caractère personnel qui la communique, le cas échéant, à une des personnes mentionnées ci-dessus ([108]).

En cas de remise de la demande sur place, la personne qui la reçoit délivre immédiatement un accusé de réception daté et signé à l'auteur de la demande ([109]).

Dans le mois qui suit l'introduction de la requête, le responsable du traitement communique les rectifications ou effacements des données, effectués sur base de l'article 12, § 1, de la loi du 8 décembre 1992. Cette communication doit être adressée à la personne concernée ainsi qu'aux personnes à qui les données ont été communiquées, pour autant qu'il ait encore connaissance des destinataires de la communication et que la notification à ces destinataires ne paraisse pas impossible ou n'implique pas des efforts disproportionnés ([110]).

Dès la réception de la demande de suppression ou d'interdiction d'utilisation, le responsable du traitement doit indiquer clairement, lors de toute communication, que la donnée est contestée (art. 15 de la loi du 8 décembre 1992). Le non-respect de cette obligation est passible d'une amende de 100 à 20.000 EUR (+ application des décimes additionnels).

10.1.3.4.8. Le droit d'obtenir, sans frais, la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel la concernant qui a été conservée au-delà de la période autorisée ([111])

Toute personne a le droit d'obtenir sans frais la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel la concernant qui a été conservée au-delà de la période autorisée (art. 12, § 1er, al. 5, de la loi du 8 décembre 1992).

Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement ([112]).

Pour obtenir la rectification, la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel qui a été conservée au-delà de la période autorisée ([113]), sans frais à sa

---

108 Art. 32, al. 1, de l'arrêté royal du 13 février 2001.

109 Art. 32, al. 2, de l'arrêté royal du 13 février 2001.

110 Art. 12, § 3, al. 1, de la loi du 8 décembre 1992.

111 Art. 12, § 1, al. 5, de la loi du 8 décembre 1992.

112 Art. 4, § 1, 5°, de la loi du 8 décembre 1992. Le Roi a prévu les garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques, dans l'arrêté royal du 13 février 2001.

113 La procédure est fixée par l'art. 12, §§ 2 et 3, de la loi du 8 décembre 1992, précisée par l'art. 33 de l'arrêté royal du 13 février 2001 précité (qui renvoie à la procédure déterminée à l'art. 32). Voyez aussi à ce sujet : C. de TERWANGNE et S. LOUVEAUX, o.c., *J.T.*, 2001, p. 461 et s.

charge ([114]), la personne concernée doit justifier son identité et adresser une demande datée et signée qu'elle remet sur place ou qu'elle envoie par la poste ou par tout moyen de télécommunication, soit au responsable du traitement ou à son représentant en Belgique ou à l'un de ses mandataires ou préposés, soit au sous-traitant du traitement des données à caractère personnel qui la communique, le cas échéant, à une des personnes mentionnées ci-dessus ([115]).

En cas de remise de la demande sur place, la personne qui la reçoit délivre immédiatement un accusé de réception daté et signé à l'auteur de la demande ([116]).

Dans le mois qui suit l'introduction de la requête, le responsable du traitement communique les rectifications ou effacements des données, effectués sur base de l'article 12, § 1, de la loi du 8 décembre 1992. Cette communication doit être adressée à la personne concernée ainsi qu'aux personnes à qui les données incorrectes ont été communiquées, pour autant qu'il ait encore connaissance des destinataires de la communication et que la notification à ces destinataires ne paraisse pas impossible ou n'implique pas des efforts disproportionnés ([117]).

Dès la réception de la demande de suppression ou d'interdiction d'utilisation, le responsable du traitement doit indiquer clairement, lors de toute communication, que la donnée est contestée (art. 15 de la loi du 8 décembre 1992). Le non-respect de cette obligation est passible d'une amende de 100 à 20.000 EUR (+ application des décimes additionnels).

10.1.3.4.9. Le droit de ne pas être soumis à une décision automatisée

La loi prévoit qu'une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité ([118]). Dans un hôpital, cela vise par exemple la vérification de l'assurabilité d'un patient à l'aide de la carte SIS.

Toutefois, cette interdiction ne s'applique pas lorsque la décision est prise dans le cadre d'un contrat ou est fondée sur une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance. Ce contrat ou cette disposition doivent contenir des mesures appropriées, garantissant la sauvegarde des intérêts légitimes de l'intéressé. Il devra au moins être permis à celui-ci de faire valoir utilement son point de vue ([119]).

---

114 Art. 12, § 1, al. 5, de la loi du 8 décembre 1992.
115 Art. 32, al. 1, de l'arrêté royal du 13 février 2001.
116 Art. 32, al. 2, de l'arrêté royal du 13 février 2001.
117 Art. 12, § 3, al. 1, de la loi du 8 décembre 1992.
118 Art. 12 bis, al. 1, de la loi du 8 décembre 1992.
119 Art. 12 bis, al. 2, de la loi du 8 décembre 1992.

10.1.3.4.10. Le recours comme en référé

Afin d'assurer une protection particulière à la personne concernée ([120]), la loi du 8 décembre 1992 a créé un recours juridictionnel spécifique auprès du président du tribunal de première instance siégeant *comme en référé* ([121]) mais *statuant au fond* ([122]). Pour relever de sa compétence, les demandes doivent soit ([123]) :

1° être relatives au droit de la personne concernée d'obtenir communication de ses données à caractère personnel, que ce droit soit accordé par ou en vertu de la loi ;
2° tendre à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel inexacte ;
3° tendre à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel incomplète ou non pertinente, compte tenu du but du traitement ;
4° tendre à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel dont l'enregistrement, la communication ou la conservation sont interdits ;
5° tendre à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel au traitement de laquelle la personne concernée s'est opposée ;
6° tendre à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel qui a été conservée au-delà de la période autorisée.

Il faut immédiatement attirer l'attention sur le fait que cette procédure *comme en référé* n'a pas pour objet de soumettre l'ensemble du traitement de données à un contrôle de légalité. Autrement dit, la personne concernée ne peut pas introduire une demande qui porte sur la légalité ou sur la totalité du système d'information en tant que tel ([124]) ; sa demande ne peut porter sur celui-ci que dans la mesure où ce dernier la concerne ([125]). C'est en ce sens que le recours créé au profit de la personne concernée a pour objet la protection de ses droits subjectifs et non pas un véritable contrôle de légalité ([126]).

---

120 Doc. Parl., Ch., s.e., 1991/1992, n° 413/12, p. 11 : « *Le projet de loi prévoit une technique particulière de protection en accordant au titulaire qui n'obtient pas satisfaction du maître du fichier, un droit de recours. Ce recours peut être exercé à deux endroits : près de la Commission (article 29, § 4) ou près du tribunal (article 15).* ».

121 Art. 14 de la loi du 8 décembre 1992. L'article 587, 4°, du Code judiciaire est le reflet de l'article 14 de la loi du 8 décembre 1992 : « *Le président du tribunal de première instance statue sur les demandes prévues à l'article 14 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.* »

122 Civ. Brux. (réf.), 22 mars 1994, *J.T.*, 1994, p. 841, obs. Th. LEONARD, spéc. p. 843.

123 Art. 14, § 1, de la loi du 8 décembre 1992.

124 La personne concernée ne peut donc pas demander au Président d'ordonner la cessation de tout un fichier ou de tout un système d'information.

125 En ce sens : Civ. Brux. (réf.), 19 déc. 2000, *Bull. Ass.*, 2001 n° 335, p. 267 et s., obs. Ch.-A. van OLDENEEL, « Une décision qui donne raison à Datassur », p. 277 et s. ; *Computerrecht*, 2002/01, p. 30 et s.

126 Même si la procédure induit *de facto* un contrôle de légalité, celui-ci ne sera pas complet. Sur cette procédure, voyez not. : J. HERVEG, « La procédure "comme en référé" appliquée aux

Dès la notification de l'introduction de la procédure comme en référés, le responsable du traitement doit indiquer clairement, lors de toute communication, que la donnée est contestée (art. 15 de la loi du 8 décembre 1992). Le non-respect de cette obligation est passible d'une amende de 100 à 20.000 EUR (+ application des décimes additionnels).

10.1.3.4.11. Le droit d'obtenir, à charge du responsable du traitement, la réparation du dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la loi, sauf à ce qu'il établisse que le fait générateur ne lui est pas imputable

Le responsable du traitement est responsable du dommage causé à la personne concernée par un acte contraire aux dispositions déterminées par ou en vertu de la loi du 8 décembre 1992 (art. 15 bis de la loi du 8 décembre 1992).

Il est exonéré de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

Cette responsabilité exorbitante est sans préjudice d'actions fondées sur d'autres dispositions légales. Autrement dit, la personne concernée peut se prévaloir d'une autre base pour interpeller la responsabilité du responsable du traitement.

10.1.3.4.11. Lorsque la légitimité du traitement de données à caractère personnel se fonde sur le consentement de la personne concernée, celle-ci a le droit de retirer son consentement à tout moment sans justification ni préavis.

Nous avons vu que la loi dispose que le traitement des données à caractère personnel peut être effectué lorsque la personne concernée a indubitablement donné son consentement (art. 5, a), de la loi du 8 décembre 1992) et que l'interdiction de traiter les données médicales est levée notamment lorsque la personne concernée a donné son consentement par écrit, pour autant qu'elle puisse le retirer à tout moment (art. 7, § 2, a), de la loi du 8 décembre 1992). Cette dernière possibilité s'applique également dans la première hypothèse.

10.1.3.5. Confidentialité et sécurité des traitements de données à caractère personnel

La confidentialité et la sécurité du traitement de données à caractère personnel doivent être garanties ([127]). A ce double effet, la loi du 8 décembre 1992 impose toute une série d'obligations à charge du responsable du traitement.

---

traitements de données », in *Les actions en cessation*, Bruxelles, Larcier, Collection CUP, 2006, vol. 87, 05/2006, pp. 215-246

[127] Voyez à propos de la sécurité informatique : « La sécurité informatique, entre technique et droit », Cahiers du CRID, n° 14, 1998.

Il faut souligner l'importance de la confidentialité et de la sécurité des traitements de données à caractère personnel. Dans son arrêt du 17 juillet 2008 (I. c Finlande), la Cour européenne des droits de l'homme, saisie d'une plainte relative à l'accès à des données médicales au sein d'un hôpital, a souligné le fait qu'il n'était pas suffisant que la législation nationale prévoit que la personne concernée puisse réclamer la réparation des dommages causés par une divulgation non autorisée de données à caractère personnel, pour protéger sa vie privée. La Cour a indiqué que ce qui était requis est une protection réelle et effective qui exclut toute possibilité d'accès non autorisé aux données à caractère personnel (§ 47). Elle avait au préalable mis en exergue l'importance de deux mesures : d'abord, la restriction de l'accès aux dossiers médicaux aux professionnels de la santé directement impliqués dans la prise en charge de la personne concernée, et, ensuite, l'existence d'un fichier « log » permettant d'identifier toutes les personnes ayant accès aux dossiers médicaux. En effet, en l'espèce, ces deux mesures auraient permis de prévenir l'accès non autorisé et de dire s'il y avait eu un accès non autorisé au dossier médical de la requérante et, le cas échéant, d'identifier alors son auteur et de le poursuivre en réparation.

10.1.3.5.1. Garantir la qualité des données

Dans la droite ligne du principe relatif à la qualité des données, le responsable du traitement (ou son représentant) doit faire toute diligence pour (art. 16, § 2, 1°, de la loi du 8 décembre 1992) :

- tenir les données à jour,
- rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des articles 4 à 8 de la loi du 8 décembre 1992.

10.1.3.5.2. Police d'accès

Le responsable du traitement (ou son représentant) doit mettre en œuvre une police d'accès qui permette d'assurer que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service (art. 16, § 2, 2°, de la loi du 8 décembre 1992).

La loi prévoit aussi que toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance (art. 16, § 3, de la loi du 8 décembre 1992).

Comme indiqué ci-avant, il faut pouvoir déterminer qui peut accéder à quelles données et pour quoi faire. De plus, il faut conserver les logs de ces opérations afin de pouvoir opérer en

outre des contrôles *a posteriori* et garantir l'exercice des droits d'accès de la personne concernée et la confidentialité et la sécurité des traitements de données à caractère personnel.

10.1.3.5.3. Obligation de formation du personnel à la protection des données

Le responsable du traitement (ou son représentant) doit informer les personnes agissant sous son autorité des dispositions de la loi du 8 décembre 1992 et de ses arrêtés d'exécution, ainsi que de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel (art. 16, § 2, 3°, de la loi du 8 décembre 1992).

10.1.3.5.4. Conformité des programmes

Le responsable du traitement (ou son représentant) doit s'assurer de la conformité des programmes servant au traitement automatisé des données à caractère personnel avec les termes de la déclaration du traitement des données à notifier à la Commission de protection de la vie privée, ainsi que de la régularité de leur application (art. 16, § 2, 4°, de la loi du 8 décembre 1992).

10.1.3.5.5. Mesures techniques et organisationnelles

Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel (art. 16, § 4, al. 1, de la loi du 8 décembre 1992) ([128]).

Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels (art. 16, § 4, al. 2, de la loi du 8 décembre 1992).

Sur avis de la Commission de la protection de la vie privée, le Roi peut édicter des normes appropriées en matière de sécurité informatique pour toutes ou certaines catégories de traitements (art. 16, § 4, al. 3, de la loi du 8 décembre 1992).

De manière générale, ces mesures comprennent principalement, sans que la liste ne prétende à l'exhaustivité :

- l'identification des utilisateurs ;

---

[128] Voyez les mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel, préconisées par la Commission de protection de la vie privée (ce document est disponible sur son site Web).

- la gestion des accès aux données ;
- la gestion des pouvoirs des utilisateurs sur les données auxquelles ils peuvent accéder ;
- des antivirus ;
- des firewalls ;
- des systèmes de sauvegarde en insistant sur le fait que les copies de sauvegarde ne devraient pas être conservées dans le même bâtiment ;
- la protection de l'information qui circule dans des réseaux télématiques ouverts ou fermés notamment par le biais de son chiffrement ;
- la traçabilité des accès ;
- la traçabilité des opérations effectuées sur les données ;
- des mesures de contrôle inopinés et à intervalles réguliers par des personne ou des organismes, internes et externes, qui présentent des garanties d'indépendance ;
- l'instauration d'un groupe pluridisciplinaire représentant toutes les personnes impliquées dans le système d'information hospitalier, chargé d'une mission générale de pilotage et de surveillance.

S'agissant des hôpitaux, il est opportun de rappeler certaines des mesures énumérées dans l'annexe de l'arrêté royal du 23 octobre 1964 (9° quater) :

- la désignation d'un conseiller en sécurité chargé de la sécurité de l'information et qui conseille le responsable du traitement au sujet de tous les aspects de la sécurité de l'information ;
- les catégories de personnes ayant accès ou étant autorisées à obtenir les données médicales ;
- les catégories de personnes dont les données font l'objet d'un traitement ;
- la nature des données traitées et la manière dont elles sont obtenues ;
- l'organisation du circuit des données médicales à traiter ;
- la procédure suivant laquelle, si nécessaire, les données sont rendues anonymes ;
- les procédures de sauvegarde afin d'empêcher :
  - la destruction accidentelle ou illicite de données,
  - la perte accidentelle de données ou l'accès illicite à celles-ci,
  - leur modification ou diffusion illicite ;
- le délai au-delà duquel les données ne peuvent plus, le cas échéant, être gardées, utilisées ou diffusées ;
- les rapprochements, interconnexions ou tout autre forme de mise en relation de données l'objet du traitement ;
- les interconnexions et les consultations ;
- les cas où des données sont effacées ;
- la désignation du médecin sous la responsabilité et la surveillance duquel sont effectués les traitements de données médicales.

10.1.3.5.5. En cas d'intervention d'un sous-traitant

Lorsque l'hôpital confie tout ou partie d'un traitement de données à caractère personnel à un sous-traitant, il doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements (art. 16, § 1er, 1°, de la loi du 8 décembre 1992). Pour reprendre l'exemple des analyses sanguines confiées à un laboratoire extérieur à l'hôpital, cela signifie que l'hôpital doit au préalable s'assurer des garanties offertes par le laboratoire en matière de mesures de sécurité technique et d'organisation.

De plus, l'hôpital doit veiller au respect de ces mesures notamment par la stipulation de mentions contractuelles (art. 16, § 1er, 2°, de la loi du 8 décembre 1992) et fixer dans le contrat la responsabilité du sous-traitant à l'égard du responsable du traitement (art. 16, § 1er, 3°, de la loi du 8 décembre 1992).

L'hôpital doit aussi convenir avec son sous-traitant que celui-ci n'agira que sur ses seules instructions et qu'il est tenu par les mêmes obligations que celles auxquelles l'hôpital est lui-même tenu en matière de police d'accès et d'utilisation des données. Ainsi, pour rappel, toute personne agissant sous l'autorité du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance (art. 16, § 1er, 4°, de la loi du 8 décembre 1992).

Enfin, l'hôpital doit consigner par écrit ou sur un support électronique les éléments du contrat relatifs à la responsabilité du sous-traitant et sur l'accès aux données relatifs à la protection des données et les exigences portant sur les mesures en matière de police d'accès et d'utilisation données (art. 16, § 1er, 5°, de la loi du 8 décembre 1992).

Le non-respect des obligations visées à l'article 16, § 1er, de la loi du 8 décembre 1992 est passible d'une amende de 100 à 20.000 EUR (+ application des décimes additionnels).

10.1.3.6. Déclaration des traitements de données à caractère personnel et Registre public près la Commission de la protection de la vie privée

10.1.3.6. Généralités

L'hôpital doit déclarer à la Commission de la protection de la vie privée les traitements de données à caractère personnel, automatisés en tout ou en partie, ou l'ensemble de tels traitements qui ont une même finalité ou des finalités liées, avant leur mise en œuvre (art. 17, § 1er, de la loi du 8 décembre 1992).

La loi précise que chaque finalité ou ensemble de finalités liées pour lesquelles il est procédé à un ou à plusieurs traitements partiellement ou totalement automatisés doit faire l'objet d'une déclaration (art. 17, § 5, de la loi du 8 décembre 1992).

La suppression d'un traitement doit également faire l'objet d'une déclaration (art. 17, § 7, de la loi du 8 décembre 1992).

L'hôpital recevra un accusé de réception dans les trois jours ouvrables (art. 17, § 2, de la loi du 8 décembre 1992).

La déclaration doit mentionner (art. 17, § 3, de la loi du 8 décembre 1992) :

1° la date de la déclaration et, le cas échéant, la mention de la loi, du décret, de l'ordonnance ou de l'acte réglementaire décidant la création du traitement automatisé ;
2° les nom, prénoms et adresse complète ou la dénomination et le siège du responsable du traitement et, le cas échéant, de son représentant en Belgique ;
4° la dénomination du traitement automatisé ;
5° la finalité ou l'ensemble des finalités liées du traitement automatisé ;
6° les catégories de données à caractère personnel qui sont traitées avec une description particulière des données visées aux articles 6 à 8 de la loi du 8 décembre 1992 ;
7° les catégories de destinataires à qui les données peuvent être fournies ;
8° les garanties dont doit être entourée la communication de données aux tiers ;
9° les moyens par lesquels les personnes qui font l'objet des données en seront informées, le service auprès duquel s'exercera le droit d'accès et les mesures prises pour faciliter l'exercice de ce droit ;
10° la période au-delà de laquelle les données ne peuvent plus, le cas échéant, être gardées, utilisées ou diffusées ;
11° une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement en application de l'article 16 de la loi du 8 décembre 1992 ;
12° les motifs sur lesquels le responsable du traitement fonde, le cas échéant, l'application de l'article 3, § 3, de la loi du 8 décembre 1992.

La modification d'un de ces éléments doit également faire l'objet d'une déclaration (art. 17, § 7, de la loi du 8 décembre 1992).

La déclaration peut se faire grâce à un formulaire papier ou sur un support électronique, ce qui a un impact direct sur son coût : dans le premier cas, la déclaration coûte 125 EUR contre 25 EUR dans le second cas (art. 47 et 48 de l'arrêté royal du 13 février 2001).

Pour les modifications, la contribution est de 20 EUR (art. 49 de l'arrêté royal du 13 février 2001).

Dans le cadre de ses pouvoirs de contrôle et d'enquête visés aux articles 31 et 32 de la loi du 8 décembre 1992, la Commission de la protection de la vie privée a le pouvoir d'exiger d'autres éléments d'information, notamment l'origine des données à caractère personnel, la technique

d'automatisation choisie et les mesures de sécurité prévues (art. 17, § 4, de la loi du 8 décembre 1992).

Lorsque la Commission de la protection de la vie privée estime qu'un traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier est susceptible de porter atteinte à la vie privée, elle peut soit d'office, soit sur requête d'une personne concernée enjoindre au responsable du traitement (ici l'hôpital) de lui communiquer tout ou partie de ces informations (art. 19 de la loi du 8 décembre 1992) ([129]).

Le non-respect de l'obligation de déclarer le traitement à la Commission de protection de la vie privée est passible d'une amende de 100 à 100.000 EUR (+ application des décimes additionnels).

10.1.3.6.2. Exemptions à l'obligation de déclaration

Moyennant le respect de conditions spécifiques, un certain nombre de traitements sont exemptés de l'obligation de déclaration, ce qui ne les soustrait évidemment pas au reste de la loi du 8 décembre 1992. Ces traitements sont énumérés aux articles 51 à 62 de l'arrêté royal du 13 février 2001. Cela concerne essentiellement :

- l'administration des salaires ;
- l'administration du personnel ;
- la comptabilité du responsable du traitement ;
- l'administration des actionnaires et des associés ;
- la gestion de la clientèle ou des fournisseurs du responsable du traitement ;
- l'administration par une fondation, une association ou tout autre organisme sans but lucratif dans le cadre de ses activités ordinaires, des membres, des bienfaiteurs ou des personnes avec qui le responsable du traitement est en contact régulier ;
- aux traitements de données d'identification indispensables à la communication effectués dans le seul but d'entrer en contact avec l'intéressé ;
- l'enregistrement des visiteurs dans le cadre d'un contrôle d'accès ;
- les traitements de données à caractère personnel effectués par les établissements d'enseignement en vue de gérer leurs relations avec leurs élèves ou étudiants ;
- les traitements effectués par les Communes en matière de registres de la population, de cartes d'identité, de législation électorale et de registres de l'état civil ;
- les traitements de données à caractère personnel effectués par des autorités administratives si le traitement est soumis à des réglementations particulières adoptées par ou en vertu de la loi et réglementant l'accès aux données traitées ainsi que leur utilisation et leur obtention ;

---

[129] Voyez aussi la situation particulière visée à l'article 20 de la loi du 8 décembre 1992.

- les traitements de données à caractère personnel gérés par les institutions de sécurité sociale.

10.1.3.6.3. La consultation du Registre public

Tout le monde, en ce compris le patient, a le droit de consulter le Registre public tenu par la Commission de la protection de la vie privée. Ce registre contient des informations relatives aux traitements entièrement ou partiellement automatisés de données à caractère personnel qui lui sont déclarés (art. 18 de la loi du 8 décembre 1992).

Le patient peut consulter le registre directement sur place, ou par le biais de moyens de télécommunication, ou encore par une demande d'extrait adressée en ce sens à la Commission (art. 63 et s. de l'arrêté royal du 13 février 2001).

En tout état de cause, la consultation est gratuite et ne doit pas être motivée (art. 68 et 69 de l'arrêté royal du 13 février 2001).

S'agissant de traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier, lorsque la Commission estime qu'il est susceptible de porter atteinte à la vie privée, elle peut, soit d'office, soit à la requête de la personne concernée, enjoindre au responsable du traitement de lui communiquer tout ou partie des informations faisant l'objet de la déclaration des traitements entièrement ou partiellement automatisés (art. 19 de la loi du 8 décembre 1992).

10.1.3.7. Transferts de données à caractère personnel hors Union européenne

10.1.3.7.1. L'exigence d'un niveau de protection adéquat

Le transfert de données à caractère personnel faisant l'objet d'un traitement après leur transfert vers un pays non membre de la Communauté européenne, ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions de la présente loi et de ses arrêtés d'exécution (art. 21, § 1er, al. 1, de la loi du 8 décembre 1992).

Le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts de données. Il est notamment tenu compte (art. 21, § 1er, al. 2, de la loi du 8 décembre 1992) :

- de la nature des données,
- de la finalité et de la durée du ou des traitements envisagés,
- des pays d'origine et de destination finale,
- des règles de droit, générales et sectorielles, en vigueur dans le pays en cause,
- des règles professionnelles,

- et des mesures de sécurité qui y sont respectées.

10.1.3.7.2. Les dérogations à l'exigence d'un niveau de protection adéquat et le recours aux clauses contractuelles

La loi du 8 décembre 1992 prévoit toute une série d'hypothèses dans lesquelles nonobstant l'absence d'un niveau de protection adéquat, il est néanmoins possible de transférer des données à caractère personnel :

1° la personne concernée a indubitablement donné son consentement au transfert envisagé ;
2° le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou des mesures préalables à la conclusion de ce contrat, prises à la demande de la personne concernée ;
3° le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ;
4° le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice ;
5° le transfert est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ;
6° le transfert intervient au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

En outre, le Roi peut, après avis de la Commission de la protection de la vie privée, autoriser un transfert ou un ensemble de transferts de données à caractère personnel vers un pays non membre de la Communauté européenne et n'assurant pas un niveau de protection adéquat, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants. La loi du 8 décembre 1992 indique que ces garanties peuvent notamment résulter de clauses contractuelles appropriées. A cet effet, il est utile de se référer aux deux décisions suivantes de la Commission européenne :

- Décision 2001/497/CE de la Commission du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE, telle que modifiée par la Décision 2004/915/CE de la Commission du 27 décembre 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers.

- Décision 2002/16/CE de la Commission du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans pays tiers en vertu de la directive 95/46/CE.

10.1.3.8. La Commission de la protection de la vie privée et les Comités sectoriels

10.1.3.8.1. La Commission de la protection de la vie privée

La Commission de la protection de la vie privée est instituée auprès de la Chambre des Représentants (art. 23 de la loi du 8 décembre 1992).

10.1.3.8.1.1. Les missions de la Commission de la protection de la vie privée

La Commission de la protection de la vie privée émet des avis et formule des recommandations à l'intention des autorités et/ou instances compétentes (voyez les articles 29 et 30 de la loi du 8 décembre 1992).

La personne concernée peut aussi se plaindre auprès de la Commission de la protection de la vie privée, dans la mesure où cette plainte a trait à sa mission de protection de la vie privée ou à d'autres missions qui lui sont confiées par la loi ([130]). Après l'examen de la recevabilité, la Commission accomplit toute mission de médiation qu'elle juge utile. En l'absence de conciliation, elle émet un avis motivé sur le caractère fondé de la plainte. Cet avis peut, le cas échéant, être accompagné de recommandations motivées à l'intention du responsable du traitement. Une copie de l'avis ou des recommandations est adressée à la personne concernée, au responsable du traitement, à toutes les parties à la cause, et au Ministre de la Justice.

10.1.3.8.1.2. Les pouvoirs de la Commission de la protection de la vie privée

Pour l'accomplissement de toutes ses missions, la Commission peut requérir le concours d'experts. Elle peut charger un ou plusieurs de ses membres éventuellement assistés d'experts, de procéder à un examen sur place. Dans ce cas, les membres de la Commission ont la qualité d'officier de police judiciaire, auxiliaire du procureur du Roi. Ils peuvent notamment exiger communication de tout document pouvant leur être utile dans leur enquête. Ils peuvent également pénétrer en tous lieux où ils ont un motif raisonnable de supposer que s'exerce une activité en rapport avec l'application de la présente loi (art. 32, § 1er, de la loi du 8 décembre 1992).

La Commission dénonce au procureur du Roi les infractions dont elle a connaissance (art. 32, § 2, de la loi du 8 décembre 1992).

La loi précise que, sans préjudice de la compétence des cours et tribunaux ordinaires pour l'application des principes généraux en matière de protection de la vie privée, le Président de la Commission peut soumettre au tribunal de première instance tout litige concernant

---

130 Art. 31, de la loi du 8 décembre 1992.

l'application de la présente loi et de ses mesures d'exécution (art. 32, § 3, de la loi du 8 décembre 1992).

10.1.3.8.1.3. L'obligation au secret

Les membres et membres du personnel de la Commission ainsi que les experts dont le concours est requis sont tenus d'une obligation de confidentialité à l'égard des faits, actes ou renseignements dont ils ont eu connaissance en raison de leurs fonctions (art. 33 de la loi du 8 décembre 1992).

10.1.3.8.2. Les Comités sectoriels

10.1.3.8.2.1. Généralités

La loi du 8 décembre 1992 a créé des Comités sectoriels au sein de la Commission de la protection de la vie privée. Ceux-ci sont compétents pour instruire et statuer sur des demandes relatives au traitement ou à la communication de données faisant l'objet de législations particulières, dans les limites déterminées par celle-ci (voyez l'article 31 bis de la loi du 8 décembre 1992).

Les demandes relatives au traitement ou à la communication de données réglementées par une législation particulière, introduites auprès de la Commission, sont transmises par celle-ci au Comité sectoriel compétent, s'il a été constitué, ainsi qu'à l'institution de gestion du secteur concerné. Celle-ci transmet au Comité sectoriel un avis technique et juridique endéans les quinze jours et pour autant que le dossier soit en état. Le Comité statue, sous la même réserve, endéans les trente jours de la réception de cet avis ou, le cas échéant, de l'expiration du délai de quinze jours précité. A défaut, sa décision est réputée conforme à l'avis technique et juridique précité (art. 31 bis, § 3, de la loi du 8 décembre 1992).

10.1.3.8.2.2. Le Comité sectoriel pour l'autorité fédérale

Dans la Commission de la protection de la vie privée est créé un Comité sectoriel pour l'autorité fédérale au sens de l'article 31bis. Le Service public fédéral Technologie de l'Information et de la Communication est considéré comme étant l'institution de gestion visée à l'article 31bis pour le Comité sectoriel pour l'autorité fédérale (art. 36 bis de la loi du 8 décembre 1992).

Sauf dans les cas fixés par le Roi, toute communication électronique de données personnelles par un service public fédéral ou par un organisme public avec personnalité juridique qui relève de l'autorité fédérale, exige une autorisation de principe de ce Comité sectoriel, à moins que la communication n'ait déjà fait l'objet d'une autorisation de principe d'un autre Comité sectoriel créé au sein de la Commission de la protection de la vie privée. Avant d'octroyer son autorisation, le Comité sectoriel pour l'autorité fédérale vérifie si la communication est

conforme aux dispositions légales et réglementaires. Les autorisations fournies par le Comité sectoriel pour l'autorité fédérale sont publiques dès qu'elles sont définitives. Elles sont publiées sur le site Internet de la Commission de la protection de la vie privée (art. 36 bis de la loi du 8 décembre 1992).

10.1.3.8.2.3. Le Comité sectoriel « Sécurité sociale » et « Santé »

10.1.3.8.2.3.1. Généralités

Il existe aussi un Comité sectoriel « Sécurité sociale » et « Santé » (loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité sociale) ([131]).

Il est composé de deux sections (art. 37**, § 1er,** de la loi du 15 janvier 1990) :

- une section « Sécurité Sociale »,
- et une section « Santé ».

La loi du 15 janvier 1990 déroge à la loi du 8 décembre 1992 quant à la composition de ce Comité sectoriel (voyez **son article 37, § 2**). De plus, les deux sections sont établies et tiennent leurs réunions au siège de la Banque-Carrefour de la Sécurité sociale (art. 41 de la loi du 15 janvier 1990).

Les institutions de gestion avec lesquelles ce Comité sectoriel est en contact conformément à la législation applicable sont :

- la Banque-Carrefour de la Sécurité sociale,
- le Centre fédéral d'expertise des soins de santé,
- et la fondation visée à l'article 45quinquies de l'arrêté royal n° 78 du 10 novembre 1967 relatif à l'exercice des professions des soins de santé (en vertu duquel l'Etat peut, avec les organismes assureurs, visés dans la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, et pour les pathologies en rapport avec le cancer, créer une fondation d'utilité publique).

Dans sa mouture précédente, l'institution de gestion pour le Comité sectoriel pour les données de santé était composée par le SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement, et l'INAMI.

10.1.3.8.2.3.2. Missions des instituts de gestion du Comité sectoriel « Sécurité sociale » et « Santé »

[131] Sur le Comité sectoriel, voyez not. : Y. POULLET, « Construire un cadre juridique pour l'e-Health », o.c., p. 109, n° 19.

La Banque-Carrefour de la Sécurité sociale est chargée de rédiger l'avis technique et juridique relatif à toute demande concernant la communication de données sociales à caractère personnel dont elle a reçu une copie de la part de la section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé ou de la part de la Commission de la protection de la vie privée (art. 42, § 1, de la loi du 15 janvier 1990).

~~Le Centre fédéral d'expertise des soins de santé est, jusqu'à une date à déterminer par le Roi, chargé de rédiger l'avis technique et juridique relatif à toute demande concernant la communication de données à caractère personnel relatives à la santé au sens de la loi du 8 décembre 1992, dont il a reçu une copie de la part de la section santé du Comité sectoriel de la sécurité sociale et de la santé ou de la part de la Commission de la protection de la vie privée (art. 42, § 2, al. 1, de la loi du 15 janvier 1990).~~

~~Par dérogation à l'article 42, § 2, al. 1, de la loi du 15 janvier 1990, la fondation visée à l'article 45quinquies de l'A.R. n° 78 est chargée de rédiger l'avis technique et juridique relatif à toute demande concernant les traitements de données à caractère personnel visées à l'article 45quinquies de l'A.R. n° 78 dont elle a saisi la section santé du Comité sectoriel de la sécurité sociale et de la santé ou la Commission de la protection de la vie privée (art. 42, § 2, al. 2, de la loi du 15 janvier 1990).~~

Conformément à l'article 31bis, § 3, de la loi précitée du 8 décembre 1992, la plate-forme eHealth, visée à l'article 2 de la loi du […] relative à l'institution et à l'organisation de la plate-forme eHealth, est chargée de rédiger l'avis technique et juridique relatif à toute demande concernant la communication de données à caractère personnel relatives à la santé au sens de la loi précitée du 8 décembre 1992, dont elle a reçu une copie de la part de la section santé du comité sectoriel de la sécurité sociale et de la santé ou de la part de la Commission de la protection de la vie privée. Le président du comité sectoriel de la sécurité sociale et de la santé ou la plate-forme eHealth peuvent décider de faire appel, pour la rédaction de l'avis technique et juridique, au soutien du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement, de l'Institut national d'assurance maladie-invalidité, du Centre fédéral d'expertise des soins de santé ou de la fondation visée à l'article 45quinquies de l'arrêté royal n° 78 du 10 novembre 1967 relatif à l'exercice des professions de soins de santé. (art. 42, § 2, de la loi du 15 janvier 1990)»

10.1.3.8.2.3.3. Prise en charge des frais de fonctionnement du Comité sectoriel « Sécurité sociale » et « Santé »

Les frais de fonctionnement des deux sections du Comité sectoriel de la sécurité sociale et de la santé sont pris en charge par la Banque-Carrefour de la Sécurité sociale, sauf les indemnités et remboursements de frais alloués à ses membres, qui sont pris en charge par la Commission de la protection de la vie privée et des frais de rédaction des avis techniques et juridiques du

Centre fédéral d'expertise des soins de santé ou de la fondation (art. 43 de la loi du 15 janvier 1990).

10.1.3.8.2.3.4. Compétences de la section « Sécurité sociale »

Sauf si la loi en dispose autrement, la section sécurité sociale est compétente pour l'examen des dossiers concernant le traitement, par les institutions de sécurité sociale et les personnes auxquelles tout ou partie des droits et obligations résultant de la loi du 15 janvier 1990 et de ses mesures d'exécution a été étendu en application de l'article 18, de données à caractère personnel au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, ainsi que pour l'examen de dossiers concernant le traitement de données sociales à caractère personnel par les instances d'octroi visées à l'article 11bis (art. 43 bis de la loi du 15 janvier 1990).

10.1.3.8.2.3.5. Compétences de la section « Santé »

Sauf si la loi en dispose autrement, la section santé est compétente pour l'examen des dossiers concernant le traitement de données à caractère personnel relatives à la santé au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, sauf en ce qui concerne les traitements de données à caractère personnel relatives à la santé effectués par les institutions de sécurité sociale et les personnes auxquelles tout ou partie des droits et obligations résultant de la loi du 15 janvier 1990 et de ses mesures d'exécution a été étendu en application de l'article 18 et les traitements de données sociales à caractère personnel relatives à la santé effectués par les instances d'octroi visées à l'article 11bis (art. 43 bis de la loi du 15 janvier 1990).

10.1.3.8.2.3.6. Réunion commune des deux sections

Si un dossier relève des compétences des deux sections, il est examiné au cours d'une réunion commune de celles-ci (art. 43 bis de la loi du 15 janvier 1990). Le Président du Comité sectoriel de la sécurité sociale et de la santé est chargé, en concertation avec les membres visés à l'article 37, § 2, 2° et 5°, de la loi du 15 janvier 1990, de la coordination des activités des sections. Ils peuvent décider qu'un dossier sera traité conjointement par les deux sections (art. 43 bis de la loi du 15 janvier 1990).

10.1.3.8.2.3.7. Rôle du Président du Comité Sectoriel

Le Président du Comité sectoriel de la sécurité sociale est chargé, en concertation avec le membre visé à l'article 37, § 2, 2°, de la loi du 15 janvier 1990, de la coordination entre les activités du Comité sectoriel de la sécurité sociale et de la santé et celles de la Commission de la protection de la vue privée. Il veille à la comptabilité des projets de décisions soumis au Comité sectoriel avec les principes et les normes en matière de protection de la vie privée (art. 44 de la loi du 15 janvier 1990).

A cet effet, il peut décider d'ajourner un avis, une décision ou une recommandation et de soumettre au préalable la question à la Commission de la protection de la vie privée (art. 44, de la loi du 15 janvier 1990). Lors d'une telle décision, la discussion du dossier au sein du Comité sectoriel de la sécurité sociale est suspendue et le dossier est immédiatement porté à la connaissance de la Commission (art. 44 de la loi du 15 janvier 1990). A dater de la réception du dossier, la Commission de protection de la vie privée dispose d'un délai d'un mois pour communiquer son avis au Comité sectoriel de la sécurité sociale. Si ce délai n'est pas respecté, le Comité sectoriel de la sécurité sociale émet son avis, sa décision ou sa recommandation sans attendre l'avis de la Commission de protection de la vie privée (art. 44 de la loi du 15 janvier 1990). Le point de vue de la Commission de protection de la vie privée est explicitement mentionné dans l'avis, la décision ou la recommandation du Comité sectoriel de la sécurité sociale. Le cas échéant, le Comité sectoriel motive explicitement les raisons pour lesquelles le point de vue de la Commission de protection de la vie privée n'a pas du tout ou n'a partiellement pas été suivi (art. 44 de la loi du 15 janvier 1990).

10.1.3.8.2.3.8. Voix consultatives

L'administrateur général ou l'administrateur général adjoint de la Banque-Carrefour, ainsi que, le cas échéant, sur invitation du Comité, le Président du Comité général de Coordination, assistent, avec voix consultative, aux séances du Comité sectoriel de la sécurité sociale et de la santé (art. 45**, al. 2,** de la loi du 15 janvier 1990).

Le fonctionnaire dirigeant de la plate-forme eHealth assiste aux réunions de la section santé du comité sectoriel de la sécurité sociale et de la santé avec voix consultative (art. 45, al. 3, de la loi du 15 janvier 1990).

~~Les fonctionnaires dirigeants du Centre fédéral d'expertise des soins de santé et de la fondation visée à l'article 45quinquies de l'arrêté royal n° 78 du 10 novembre 1967 relatif à l'exercice des professions des soins de santé, peuvent assister, avec voie consultative, aux séances de la section santé du Comité sectoriel de la sécurité sociale et de la santé en ce qui concerne le traitement des demandes pour lesquelles leur institution a rédigé un avis juridique et technique en application de l'article 42, § 2 (art. 45**, al. 3,** de la loi du 15 janvier 1990).~~

10.1.3.8.2.3.9. Tâches de la section « Sécurité sociale »

La section « Sécurité sociale » du Comité sectoriel de la sécurité sociale et de la santé est chargée, en vue de la protection de la vie privée, des tâches suivantes (art. 46, § 1, de la loi du 15 janvier 1990) :

1° Veiller au respect de la présente loi et de ses mesures d'exécution. A cet effet, il [elle] peut permettre à la Banque-carrefour, dans les conditions et limites qu'il [elle] fixe, de suspendre l'exécution par elle de l'article 13 de la loi du 15 janvier 1990 aussi

longtemps que les institutions de sécurité sociale n'exécutent pas leur obligation de communiquer les données sociales, conformément à l'article 10 de la loi du 15 janvier 1990 A cet effet, il [elle] instruit toute demande, notamment d'enquête, émanant de la Commission de la protection de la vie privée. A cet effet, il [elle] peut déclarer aux inspecteurs sociaux visés à l'article 53 de la loi du 15 janvier 1990 tous les cas qui constituent ou laissent présumer une infraction ;

2° Formuler toutes recommandations qu'il [elle] juge utiles pour l'application et le respect de la présente loi et de ses mesures d'exécution ;

3° Aider à la solution de tout problème de principe ou de tout litige relatif à l'application de la présente loi et de ses mesures d'exécution ainsi que de trancher, s'il y a lieu, les litiges qui n'ont pu être résolus autrement ;

4° Donner son avis conformément à l'article 5 ;

5° Dispenser, conformément à l'article 12, alinéa 2, les institutions de sécurité sociale de passer par la Banque-carrefour pour obtenir les données sociales disponibles dans le réseau ou en vérifier l'exactitude ;

6° Autoriser toute communication de données sociales a caractère personnel, conformément à l'article 15 ;

6°bis Tenir à jour un relevé qui contient, d'une part, pour ce qui concerne chaque traitement automatisé de données à caractère personnel effectué, par une institution de sécurité sociale, en vue de l'application de la sécurité sociale, au moins les données visées à l'article 17, § 3, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, telles que communiquées ou validées par l'institution de sécurité sociale concernée, et, d'autre part, les communications autorisées en vertu de l'article 15, ainsi que celles dont la section sécurité sociale du comité sectoriel de la sécurité sociale et de la santé doit être informé, conformément au même article 15. Le Roi fixe les modalités selon lesquelles toute personne intéressée peut consulter cette liste auprès de la Banque-Carrefour ;

7° Donner son avis pour la désignation du conseiller en sécurité de la Banque-carrefour, conformément à l'article 24, alinéa 2 ;

8° Vérifier si les conseillers en sécurité reçoivent la formation permanente adéquate et travaillent de façon coordonnée. A défaut, prendre toutes mesures utiles pour assurer cette formation adéquate ou réaliser la coordination, notamment technique ;

9° Faire un rapport aux Chambres législatives chaque année, pour le premier jour de la session ordinaire, sur l'exécution de ses missions au cours de l'année écoulée et d'y annexer le relevé dont il est question au 6° ci-dessus. Ce rapport est imprimé et adressé au Roi, aux Ministres qui ont la sécurité sociale dans leurs attributions, au Comité de gestion de la Banque-carrefour, à la Commission de la protection de la vie privée et aux membres des commissions des Affaires sociales des Chambres législatives. Il peut être consulté ou acquis par toute personne intéressée.

10.1.3.8.2.3.10. Tâches de la section « Santé »

La section santé du comité sectoriel de la sécurité sociale et de la santé est chargée d'autoriser la communication de données à caractère personnel relatives à la santé au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, **pour autant que celle-ci soit rendue obligatoire en vertu de l'article 42** de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé ou d'une autre disposition fixée par ou en vertu de la loi. Elle tient à jour un relevé des communications pour lesquelles elle a accordé une autorisation (art. 46, § 2, de la loi du 15 janvier 1990).

En vue de protéger la vie privée, la section « Santé » du Comité sectoriel de la sécurité sociale et de la santé visée à l'article 37 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, dispose des compétences suivantes (art. 42, § 2, de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé) :

1° Accorder une autorisation de principe de mettre à la disposition de tiers des données personnelles, visées à l'article 86 de la loi relative aux hôpitaux, coordonnée le 7 août 1987 (situation financière, résultats d'exploitation, rapport d'audit (art. 82), renseignements statistiques, identité du directeur et/ou de la personne chargée de communiquer ces données) ;

2° Pour ce qui concerne l'enregistrement visé à l'article 45 quinquies de l'arrêté royal n° 78 du 10 novembre 1967 relatif à l'exercice des professions de santé (cancer), accorder l'autorisation pour :
   a) le couplage des données à caractère personnel de la Fondation à des données externes ;
   b) la transmission de la copie codée de données en matière d'enregistrement du cancer au Centre fédéral d'expertise des soins de santé, à l'Institut national d'assurance maladie invalidité et à l'Agence intermutualiste ;
   c) le transfert des données visées au b) à d'autres instances à des fins de recherche et sur la base d'un protocole de recherche qui satisfait aux règles fixées par le Roi.

3° Accorder une autorisation de principe pour toute communication de données à caractère personnel relatives à la santé au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, sauf dans les cas suivants :
   - si la communication est effectuée entre des professionnels des soins de santé qui sont tenus au secret professionnel et qui sont associés en personne à l'exécution des actes de diagnostic, de prévention ou de prestation de soins à l'égard du patient;
   - si la communication est autorisée par ou en vertu d'une loi, d'un décret ou d'une ordonnance, après avis de la Commission de la protection de la vie privée;

- dans les cas prévus à l'article 15, § 2, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, pour autant que la section sécurité sociale du comité sectoriel de la sécurité sociale et de la santé est compétente;
- dans les cas déterminés par le Roi, par arrêté délibéré en Conseil des Ministres, après avis de la Commission de la protection de la vie privée.

10.1.3.8.2.3.11. Pouvoirs du Comité sectoriel

Dans le cadre de l'exécution de ses tâches, le Comité sectoriel de la sécurité sociale et de la santé peut procéder à des enquêtes, charger un ou plusieurs de ses membres d'effectuer de telles enquêtes sur place et faire appel à des experts. Le Comite ou ses membres, éventuellement assistés d'experts, disposent en ce cas, aux mêmes conditions, des pouvoirs d'investigation qui sont reconnus aux agents chargés de la surveillance pénale de la présente loi et de ses mesures d'exécution. Ils peuvent notamment exiger communication de tout document pouvant leur être utile dans leur enquête. Ils peuvent également pénétrer en tous lieux où ils peuvent avoir un motif raisonnable de supposer que s'exerce une activité en rapport avec l'application de la sécurité sociale, au sens de la présente loi. Le Président du Comité sectoriel de la sécurité sociale et de la santé ainsi que les autres membres du Comité ou les experts associés sont soumis au secret professionnel visé à l'article 28 pour tout ce dont ils ont pu avoir connaissance en raison de leurs fonctions (art. 47 de la loi du 15 janvier 1990).

Le Comité sectoriel de la sécurité sociale et de la santé agit soit d'initiative, soit à la demande notamment de la Commission de la protection de la vie privée, soit à la suite d'une demande d'avis ou d'une plainte qui lui est adressée. Lorsque la doléance ou la requête est adressée à la Commission, celle-ci en saisit sans tarder le Comité sectoriel de la sécurité sociale et de la santé (art. 48 de la loi du 15 janvier 1990).

10.1.3.8.2.3.12. Coopération forcée ou volontaire et suivi des réclamations

La Banque-Carrefour de la Sécurité sociale, les institutions de sécurité sociale et les personnes amenées à participer à l'application de la sécurité sociale sont tenues de fournir toutes informations au Comité sectoriel de la sécurité sociale et de la santé ou à ses membres chargés d'enquête et de leur prêter leur concours. Les autorités hiérarchiques, quelles qu'elles soient, les employeurs, leurs préposés ou mandataires doivent autoriser leurs agents, préposés ou travailleurs à répondre aux questions qui leur sont posées dans le cadre d'une enquête par le Comité sectoriel de la sécurité sociale et de la santé ou par l'un de ses membres, et à donner suite à leurs demandes ou convocations (art. 48 de la loi du 15 janvier 1990).

Toute personne, en particulier tout membre du personnel de la Banque-carrefour, d'une institution de sécurité sociale, d'une administration ou d'un service public quel qu'il soit peut, sans avoir à obtenir d'autorisation préalable, s'adresser au Comité sectoriel de la sécurité sociale et de la santé pour lui signaler les faits ou situations qui selon son sentiment,

nécessitent l'intervention de celui-ci ou lui faire toutes suggestions utiles. Sauf accord exprès de la personne qui s'est adressée à lui, le Comité sectoriel de la sécurité sociale et de la santé ne peut en révéler le nom et il ne peut davantage révéler à quiconque qu'il a été saisi par cette voie (art. 49 de la loi du 15 janvier 1990).

Le Président du Comité sectoriel de la sécurité sociale et de la santé informe, dans un délai raisonnable, les auteurs de doléances, requêtes ou suggestions, du suivi donné à leur intervention et leur fait part des motifs qui justifient la position du Comité sectoriel de la sécurité sociale et de la santé ou, le cas échéant, celle de la Commission de la protection de la vie privée (art. 50 de la loi du 15 janvier 1990).

Lorsque le Comité sectoriel de la sécurité sociale et de la santé formule une recommandation écrite, résout un problème ou tranche une contestation, il doit être informé de la suite qui a été réservée à son intervention. A défaut de réponse satisfaisante dans le délai fixé par le Comité sectoriel de la sécurité sociale et de la santé, il peut à tout moment rendre publique la recommandation et la décision. Le destinataire de la recommandation ou de la décision peut en ce cas rendre également publique sa réponse et la décision finalement prise (art. 51 de la loi du 15 janvier 1990).

Sans préjudice de la compétence des cours et tribunaux ordinaires pour l'application des principes généraux en matière de protection de la vie privée, le Président du Comité sectoriel de la sécurité sociale et de la santé peut soumettre aux juridictions du travail tout litige concernant l'application de la présente loi et de ses mesures d'exécution (art. 52 de la loi du 15 janvier 1990).

10.1.3.9. La plate-forme eHealth

La plate-forme eHealth est chargée de rédiger l'avis technique et juridique relatif à toute demande concernant la communication de données à caractère personnel relatives à la santé au sens de la loi du 8 décembre 1992, dont elle a reçu une copie de la part de la section « Santé » du Comité sectoriel de la Sécurité sociale et de la Santé ou de la part de la Commission de la protection de la vie privée (art. 42, § 2, de la loi du 15 janvier 1990 précitée).

Le président du comité sectoriel de la sécurité sociale et de la santé ou la plate-forme eHealth peuvent décider de faire appel, pour la rédaction de l'avis technique et juridique, au soutien plusieurs institution (art. 42, § 2, de la loi du 15 janvier 1990 précitée) :

- **le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement,**
- **l'Institut national d'assurance maladie-invalidité,**
- **Le Centre fédéral d'expertise des soins de santé,**

- **La fondation visée à l'article 45quinquies de l'arrêté royal n° 78 du 10 novembre 1967 relatif à l'exercice des professions de soins de santé.**

A la date fixée par le Roi et conformément aux modalités qu'il déterminera, la plate-forme eHealth reprend les missions de la Commission « Normes en matière de télématique au service du secteur des soins de santé », cette dernière étant dissoute et son arrêté royal fondateur abrogé à la date qui sera déterminée par le Roi (art. 35 de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth).

L'Etat et l'INAMI peuvent créer, avec les organismes assureurs et les associations de prestataires de soins et d'institutions de soins, une ASBL, et ce, afin d'appuyer la promotion de la qualité de la pratique médicale et des instances chargées de cette mission par l'organisation de l'échange de données cliniques. Cette ASBL peut être chargée des missions suivantes (art. 37, al. 1er, de la loi du 21 août 2008) :

Cette association peut être chargée (art. 37, al. 3, de la loi du 21 août 2008) :

1° de déterminer l'organisation des flux de données électroniques pour la collecte, le traitement et la mise à disposition de données cliniques relatives aux prestations remboursables par l'assurance obligatoire soins de santé et indemnités et de confier l'organisation opérationnelle de ces flux de données à un ou plusieurs de ses membres ou à la plate-forme eHealth;

2° de déterminer l'organisation de registres relatifs à différents domaines cliniques et de confier l'organisation opérationnelle de ces registres à un ou plusieurs de ces membres ou à la plate-forme eHealth;

3° de recueillir des données anonymes et codées et de les mettre à la disposition du Centre fédéral d'expertise des soins de santé et d'institutions ou d'associations scientifiques en vue de la réalisation d'études scientifiques.

La loi précise que les missions de cette association ne préjudicient en rien aux compétences du Comité sectoriel de la Sécurité sociale et de la Santé en ce qui concerne l'octroi d'autorisations pour les communications de données à caractère personnel relatives à la santé (art. 37, al. 4, de la loi du 21 août 2008).

La loi précise de plus que l'ASBL ne dispose pas d'un système d'information propre pour l'échange électronique de données, la gestion de registres ou le codage et l'anonymisation de
Données (art. 38, al. 1er, de la loi du 21 août 2008). Les personnes auxquelles l'organisation opérationnelle des flux de données ou la gestion de registres est confiée en exécution de l'article 37, alinéa 3, 1° et 2°, doivent faire appel aux services de base développés par la plate-forme eHealth (art. 38, al. 2, de la loi du 21 août 2008). Le

codage et l'anonymisation des données visées à l'article 37, alinéa 3, 3°, sont opérés par la plate-forme eHealth (art. 38, al. 3, de la loi du 21 août 2008).

10.1.3.10. Communications électroniques

Loi du 13 juin 2005 relative aux communications électroniques fixe toute une série de règles relatives au secret des communications, au traitement des données et à la protection de la vie privée (art. 122 à 133).

Elle pose notamment pour principe que les communications électroniques sont confidentielles, ce qui implique la protection de leur contenu. Ceci a par exemple pour conséquence qu'il est interdit de prendre connaissance de leur contenu et de tenter d'identifier les personnes concernées (voyez l'article 124 de la loi du 13 juin 2005). Il y a bien entendu diverses exceptions à ces interdictions (voyez déjà l'article 125 de la loi du 13 juin 2005). De même, l'utilisation des données de trafic est réglementée, ce qui intéresse notamment l'exploitation des traces laissées par les internautes visitant les sites web des hôpitaux.

10.1.3.11. Caméras de vidéosurveillance

La loi du 21 mars 2007 règle l'installation et l'utilisation de caméras de surveillance. Elle fixe des conditions particulières en fonction du lieu où la caméra est installée et utilisée ; soit un lieu ouvert, soit un lieu fermé accessible au public, soit un lieu fermé non accessible au public. Il faut aussi retenir que les caméras cachées sont interdites.